10/504,097

# 日本国特許庁
# JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed h this Office.

出願年月日
ate of Application: ２００４年　３月　１日

出願番号
plication Number: 特願２００４－０５６７６４
T. 10/C] : [ＪＰ２００４－０５６７６４]

出願人
licant(s): 株式会社リコー

CERTIFIED COPY OF
PRIORITY DOCUMENT

BEST AVAILABLE COPY

２００４年　４月１２日

特許庁長官
Commissioner,
Japan Patent Office
今井康夫

出証番号　出証特２００４－３０２９７７５

【書類名】　特許願
【整理番号】　0401295
【提出日】　平成16年 3月 1日
【あて先】　特許庁長官　殿
【国際特許分類】　H04L 9/14
【発明者】
　【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
　【氏名】　榎田　寛朗
【特許出願人】
　【識別番号】　000006747
　【住所又は居所】　東京都大田区中馬込１丁目３番６号
　【氏名又は名称】　株式会社リコー
　【代表者】　桜井　正光
【代理人】
　【識別番号】　100080931
　【住所又は居所】　東京都豊島区東池袋１丁目２０番２号　池袋ホワイトハウスビル８１８号
　【弁理士】
　【氏名又は名称】　大澤　敬
【先の出願に基づく優先権主張】
　【出願番号】　特願2003- 75278
　【出願日】　平成15年 3月19日
【先の出願に基づく優先権主張】
　【出願番号】　特願2003- 96129
　【出願日】　平成15年 3月31日
【手数料の表示】
　【予納台帳番号】　014498
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9809113

【書類名】特許請求の範囲
【請求項１】
クライアントとサーバとの間で通信を確立する際にデジタル証明書を用いて認証を行い、その認証に伴って確立した通信経路で通信を行うようにしたクライアント・サーバシステムと、前記クライアント及び前記サーバと通信可能なデジタル証明書管理装置とを備えた証明書管理システムであって、
前記デジタル証明書管理装置に、
前記サーバが前記認証に使用する前記デジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手段を設け、
該証明鍵更新手段に、
更新用の新証明鍵を取得する手段と、
該新証明鍵を用いて正当性を確認可能な、前記認証に使用するための新デジタル証明書を取得する手段と、
前記新証明鍵を前記クライアントに送信する第１の送信手段と、
前記サーバのための新デジタル証明書である新サーバ証明書を前記サーバに送信する第２の送信手段とを設け、
該第２の送信手段が、前記サーバに対して前記新サーバ証明書を送信する動作を、前記クライアントから前記新証明鍵を受信した旨の情報を受信した後に行う手段であることを特徴とするデジタル証明書管理システム。
【請求項２】
請求項１記載のデジタル証明書管理システムであって、
前記デジタル証明書管理装置の前記証明鍵更新手段に、
従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって前記新証明鍵を含む証明鍵証明書を取得する手段を設け、
前記第１の送信手段は、前記新証明鍵を前記証明鍵証明書の形式で前記クライアントに送信する手段であり、
前記クライアントに、
前記デジタル証明書管理装置から前記証明鍵証明書に含まれる証明鍵を受信した場合に、受信した証明鍵証明書の正当性を従前の証明鍵を用いて確認し、そこに含まれる証明鍵が適当なものであると判断した場合に該証明鍵を記憶する手段を設けたことを特徴とするデジタル証明書管理システム。
【請求項３】
請求項１記載のデジタル証明書管理システムであって、
前記デジタル証明書管理装置の前記証明鍵更新手段に、
従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって前記新証明鍵を含む第１の証明鍵証明書を取得する手段と、
前記新証明鍵を用いて正当性を確認可能なデジタル証明書であって前記新証明鍵を含む第２の証明鍵証明書を取得する手段とを設け、
前記第１の送信手段は、前記新証明鍵を前記第１及び第２の証明鍵証明書の形式でそれぞれ前記クライアントに送信する手段であり、
前記クライアントに、
前記デジタル証明書管理装置から前記第１の証明鍵証明書を受信した場合に、該証明書の正当性を従前の証明鍵を用いて確認し、これが適当なものであると判断した場合に該証明書を記憶する手段と、
前記デジタル証明書管理装置から前記第２の証明鍵証明書を受信した場合に、該証明書の正当性を前記第１の証明鍵証明書に含まれる前記新証明鍵を用いて確認し、前記第２の証明鍵証明書が適当なものであると判断した場合に、該証明書を記憶すると共に従前の証明鍵証明書及び前記第１の証明鍵証明書を削除する手段とを設け、
前記デジタル証明書管理装置の前記第１の送信手段は、前記第２の証明鍵証明書を前記クライアントに送信する動作を、少なくとも前記サーバから前記新サーバ証明書を受信し

た旨の情報を受信した後に行う手段であることを特徴とするデジタル証明書管理システム。

【請求項４】

クライアントとサーバとの間で通信を確立する際にデジタル証明書を用いて相互認証を行い、その認証に伴って確立した通信経路で通信を行うようにしたクライアント・サーバシステムと、前記クライアント及び前記サーバと通信可能なデジタル証明書管理装置とを備えた証明書管理システムであって、

前記デジタル証明書管理装置に、

前記クライアント及び前記サーバが前記相互認証に使用する前記デジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手段を設け、

該証明鍵更新手段に、

更新用の新証明鍵を取得する手段と、

該新証明鍵を用いて正当性を確認可能な、前記相互認証に使用するための新デジタル証明書を取得する手段と、

前記クライアントのための新デジタル証明書である新クライアント証明書と、前記新証明鍵とをそれぞれ前記クライアントに送信する第１の送信手段と、

前記サーバのための新デジタル証明書である新サーバ証明書と、前記新証明鍵とをそれぞれ前記サーバに送信する第２の送信手段とを設け、

該第２の送信手段が、前記サーバに対して前記新サーバ証明書を送信する動作を、前記クライアントから前記新証明鍵を受信した旨の情報を受信した後に行う手段であり、

前記第１の送信手段が、前記クライアントに前記新クライアント証明書を送信する動作を、前記サーバから前記新証明鍵を受信した旨の情報を受信した後に行う手段であることを特徴とするデジタル証明書管理システム。

【請求項５】

請求項４記載の証明書管理システムであって、

前記第１の送信手段を、前記新証明鍵を、前記新クライアント証明書と同時あるいはそれより前に前記クライアントに送信する手段とし、

前記第２の送信手段を、前記新証明鍵を、前記新サーバ証明書と同時あるいはそれより前に前記サーバに送信する手段としたことを特徴とする証明書管理システム。

【請求項６】

クライアントとサーバとの間で通信を確立する際にデジタル証明書を用いて相互認証を行い、その認証に伴って確立した通信経路で通信を行うようにしたクライアント・サーバシステムと、前記クライアント及び前記サーバと通信可能なデジタル証明書管理装置とを備えた証明書管理システムであって、

前記デジタル証明書管理装置に、

前記クライアント及び前記サーバが前記相互認証に使用する前記デジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手段を設け、

該証明鍵更新手段に、

更新用の新証明鍵を取得する手段と、

該新証明鍵を用いて正当性を確認可能な、前記相互認証に使用するための新デジタル証明書を取得する手段と、

前記クライアントのための新デジタル証明書である新クライアント証明書と、前記新証明鍵とをそれぞれ前記クライアントに送信する第１の送信手段と、

前記サーバのための新デジタル証明書である新サーバ証明書と、前記新証明鍵とをそれぞれ前記サーバに送信する第２の送信手段とを設け、

前記第１の送信手段が、前記新クライアント証明書と前記新証明鍵とを同時に前記クライアントに送信する手段であり、

前記第２の送信手段が、前記クライアントから前記新証明鍵を受信した旨の情報を受信した後で、前記新サーバ証明書と前記新証明鍵とを同時に前記サーバに送信する手段であることを特徴とするデジタル証明書管理システム。

【請求項７】
前記サーバに、前記デジタル証明書管理装置と前記クライアントとの間の通信を仲介する手段を設け、
前記デジタル証明書管理装置と前記クライアントとは前記サーバを介して通信を行い、
該サーバが、前記デジタル証明書管理装置の第１の送信手段が前記クライアントに対して送信する新証明鍵及び／又は新クライアント証明書を、前記クライアントとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で前記クライアントに送信するようにしたことを特徴とする請求項１乃至６のいずれか一項記載のデジタル証明書管理システム。
【請求項８】
前記クライアントに、前記デジタル証明書管理装置と前記サーバとの間の通信を仲介する手段を設け、
前記デジタル証明書管理装置と前記サーバとは前記クライアントを介して通信を行い、
該クライアントが、前記デジタル証明書管理装置の第２の送信手段が前記サーバに対して送信する新証明鍵及び／又は新サーバ証明書を、前記サーバとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で前記サーバに送信するようにしたことを特徴とする請求項１乃至６のいずれか一項記載のデジタル証明書管理システム。
【請求項９】
請求項１乃至８のいずれか一項記載のデジタル証明書管理システムであって、
前記クライアントと前記サーバが行う認証は、ＳＳＬ又はＴＬＳのプロトコルに従った認証であり、
前記サーバ証明書は前記サーバの公開鍵証明書であることを特徴とするデジタル証明書管理システム。
【請求項１０】
クライアント・サーバシステムを構成するクライアント及びサーバと通信可能なデジタル証明書管理装置であって、
前記クライアントと前記サーバとの間で通信を確立する際の認証に前記サーバが使用するデジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手段を設け、
該証明鍵更新手段に、
更新用の新証明鍵を取得する手段と、
該新証明鍵を用いて正当性を確認可能な、前記認証に使用するための新デジタル証明書を取得する手段と、
前記新証明鍵を前記クライアントに送信する第１の送信手段と、
前記サーバのための新デジタル証明書である新サーバ証明書を前記サーバに送信する第２の送信手段とを設け、
該第２の送信手段が、前記サーバに対して前記新サーバ証明書を送信する動作を、前記クライアントから前記新証明鍵を受信した旨の情報を受信した後に行う手段であることを特徴とするデジタル証明書管理装置。
【請求項１１】
請求項１０記載のデジタル証明書管理装置であって、
前記証明鍵更新手段に、従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって前記新証明鍵を含む証明鍵証明書を取得する手段を設け、
前記第１の送信手段が、前記新証明鍵を前記証明鍵証明書の形式で前記クライアントに送信してここに含まれる証明鍵を記憶するよう要求する手段であることを特徴とするデジタル証明書管理装置。
【請求項１２】
請求項１０記載のデジタル証明書管理装置であって、
前記証明鍵更新手段に、
従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって前記新証明鍵を含む

第１の証明鍵証明書を取得する手段と、
前記新証明鍵を用いて正当性を確認可能なデジタル証明書であって前記新証明鍵を含む第２の証明鍵証明書を取得する手段とを設け、
前記第１の送信手段が、前記新証明鍵を前記第１及び第２の証明鍵証明書の形式でそれぞれ前記クライアントに送信する手段であって、前記クライアントに、前記第２の証明鍵証明書を記憶する場合には従前の証明鍵証明書及び前記第１の証明鍵証明書を削除させる手段を有し、前記第２の証明鍵証明書を前記クライアントに送信する動作を、少なくとも前記サーバから前記新サーバ証明書を受信した旨の情報を受信した後に行うようにしたことを特徴とするデジタル証明書管理装置。
【請求項１３】
クライアント・サーバシステムを構成するクライアント及びサーバと通信可能なデジタル証明書管理装置であって、
前記クライアントと前記サーバとの間で通信を確立する際の相互認証に使用するデジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手段を設け、
該証明鍵更新手段に、
更新用の新証明鍵を取得する手段と、
該新証明鍵を用いて正当性を確認可能な、前記相互認証に使用するための新デジタル証明書を取得する手段と、
前記クライアントのための新デジタル証明書である新クライアント証明書と、前記新証明鍵とをそれぞれ前記クライアントに送信する第１の送信手段と、
前記サーバのための新デジタル証明書である新サーバ証明書と、前記新証明鍵とをそれぞれ前記サーバに送信する第２の送信手段とを設け、
該第２の送信手段が、前記サーバに対して前記新サーバ証明書を送信する動作を、前記クライアントから前記新証明鍵を受信した旨の情報を受信した後に行う手段であり、
前記第１の送信手段が、前記クライアントに前記新クライアント証明書を送信する動作を、前記サーバから前記新証明鍵を受信した旨の情報を受信した後に行う手段であることを特徴とするデジタル証明書管理装置。
【請求項１４】
クライアント・サーバシステムを構成するクライアント及びサーバと通信可能なデジタル証明書管理装置であって、
前記クライアントと前記サーバとの間で通信を確立する際の相互認証に使用するデジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手段を設け、
該証明鍵更新手段に、
更新用の新証明鍵を取得する手段と、
該新証明鍵を用いて正当性を確認可能な、前記相互認証に使用するための新デジタル証明書を取得する手段と、
前記クライアントのための新デジタル証明書である新クライアント証明書と、前記新証明鍵とをそれぞれ前記クライアントに送信する第１の送信手段と、
前記サーバのための新デジタル証明書である新サーバ証明書と、前記新証明鍵とをそれぞれ前記サーバに送信する第２の送信手段とを設け、
前記第１の送信手段が、前記新クライアント証明書と前記新証明鍵とを同時に前記クライアントに送信する手段であり、
前記第２の送信手段が、前記クライアントから前記新証明鍵を受信した旨の情報を受信した後で、前記新サーバ証明書と前記新証明鍵とを同時に前記サーバに送信する手段であることを特徴とするデジタル証明書管理装置。
【請求項１５】
前記クライアントとは前記サーバを介して通信を行い、
該サーバは、前記第１の送信手段が前記クライアントに対して送信する新証明鍵及び／又は新クライアント証明書を、前記クライアントとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で前記クライアントに送信するサーバで

あることを特徴とする請求項１０乃至１４のいずれか一項記載のデジタル証明書管理装置。

【請求項１６】

前記サーバとは前記クライアントを介して通信を行い、

該クライアントは、前記第２の送信手段が前記サーバに対して送信する新証明鍵及び／又は新サーバ証明書を、前記サーバとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で前記サーバに送信するクライアントであることを特徴とする請求項１０乃至１４のいずれか一項記載のデジタル証明書管理装置。

【請求項１７】

請求項１０乃至１６のいずれか一項記載のデジタル証明書管理装置であって、

前記認証は、ＳＳＬ又はＴＬＳのプロトコルに従った認証であり、

前記サーバ証明書は前記サーバの公開鍵証明書であることを特徴とするデジタル証明書管理装置。

【請求項１８】

クライアント・サーバシステムを構成するクライアントとサーバとの間で通信を確立する際の認証に使用するデジタル証明書を、前記クライアント及び前記サーバと通信可能なデジタル証明書管理装置によって管理するデジタル証明書管理方法であって、

前記デジタル証明書管理装置が、

前記サーバが前記認証に使用する前記デジタル証明書の正当性を確認するための証明鍵を更新し、

該証明鍵の更新を、

更新用の新証明鍵を取得する手順と、

該新証明鍵を用いて正当性を確認可能な、前記認証に使用するための新デジタル証明書を取得する手順とを実行し、

さらに、前記新証明鍵を前記クライアントに送信する第１の手順を実行し、該クライアントから該新証明鍵を受信した旨の情報を受信した後で、前記サーバのための新デジタル証明書である新サーバ証明書を前記サーバ装置に送信する第２の手順を実行することを特徴とするデジタル証明書管理方法。

【請求項１９】

請求項１８記載のデジタル証明書管理方法であって、

前記証明鍵の更新の際に、

従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって前記新証明鍵を含む証明鍵証明書を取得する手順をさらに実行し、

前記第１の手順は、前記新証明鍵を前記証明鍵証明書の形式で前記クライアントに送信する手順であり、

前記クライアントに前記証明鍵証明書を送信する場合に、該証明鍵証明書の正当性を記憶している従前の証明鍵を用いて確認させ、そこに含まれる証明鍵が適当なものであると判断した場合に該証明鍵を記憶させることを特徴とするデジタル証明書管理方法。

【請求項２０】

請求項１８記載のデジタル証明書管理方法であって、

前記証明鍵の更新の際に、

従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって前記新証明鍵を含む第１の証明鍵証明書を取得する手順と、

前記新証明鍵を用いて正当性を確認可能なデジタル証明書であって前記新証明鍵を含む第２の証明鍵証明書を取得する手順とをさらに実行し、

前記第１の手順において、前記新証明鍵を前記第１の証明鍵証明書の形式で前記クライアントに送信し、

前記第２の手順の完了後、少なくとも前記サーバから前記新サーバ証明書を受信した旨の情報を受信した後に、前記第２の証明鍵証明書を前記クライアントに送信する手順を実行し、

前記クライアントに前記第１の証明鍵証明書を送信する際に、該証明書の正当性を従前の証明鍵を用いて確認させ、これが適当なものであると判断した場合に該証明書を記憶させ、

前記クライアントに前記第２の証明鍵証明書を送信する際に、該証明書の正当性を前記第１の証明鍵証明書に含まれる前記新証明鍵を用いて確認させ、前記第２の証明鍵証明書が適当なものであると判断した場合に、該証明書を記憶させると共に従前の証明鍵証明書及び前記第１の証明鍵証明書を削除させることを特徴とするデジタル証明書管理方法。

【請求項２１】

クライアント・サーバシステムを構成するクライアントとサーバとの間で通信を確立する際の相互認証に使用するデジタル証明書を、前記クライアント及び前記サーバと通信可能なデジタル証明書管理装置によって管理するデジタル証明書管理方法であって、

前記デジタル証明書管理装置が、

前記クライアント及び前記サーバが前記相互認証に使用する前記デジタル証明書の正当性を確認するための証明鍵を更新し、

該証明鍵の更新を、

更新用の新証明鍵を取得する手順と、

該新証明鍵を用いて正当性を確認可能な、前記相互認証に使用するための新デジタル証明書を取得する手順とを実行し、

さらに、

前記新証明鍵を前記サーバに送信する第１の手順と、

前記新証明鍵を前記クライアントに送信する第２の手順と、

前記クライアントのための新デジタル証明書である新クライアント証明書を前記クライアントに送信する第３の手順と、

前記サーバのための新デジタル証明書である新サーバ証明書を前記サーバ装置に送信する第４の手順とを適当な順番で実行し、

このとき少なくとも、前記第４の手順を、前記第２の手順の完了後、前記クライアントから前記新証明鍵を受信した旨の情報を受信した後に、前記第３の手順を、前記第１の手順の完了後、前記サーバから前記新証明鍵を受信した旨の情報を受信した後に実行するようにしたことを特徴とするデジタル証明書管理方法。

【請求項２２】

請求項２１記載のデジタル証明書管理方法であって、

前記第３の手順を前記第２の手順と同時又はその完了後に、前記第４の手順を前記第１の手順と同時又はその完了後に実行するようにしたことを特徴とするデジタル証明書管理方法。

【請求項２３】

クライアント・サーバシステムを構成するクライアントとサーバとの間で通信を確立する際の相互認証に使用するデジタル証明書を、前記クライアント及び前記サーバと通信可能なデジタル証明書管理装置によって管理するデジタル証明書管理方法であって、

前記デジタル証明書管理装置が、

前記クライアント及び前記サーバが前記相互認証に使用する前記デジタル証明書の正当性を確認するための証明鍵を更新し、

該証明鍵の更新を、

更新用の新証明鍵を取得する手順と、

該新証明鍵を用いて正当性を確認可能な、前記相互認証に使用するための新デジタル証明書を取得する手順とを実行し、

さらに、

前記新証明鍵を前記サーバに送信する第１の手順と、

前記新証明鍵を前記クライアントに送信する第２の手順と、

前記クライアントのための新デジタル証明書である新クライアント証明書を前記クライアントに送信する第３の手順と、

前記サーバのための新デジタル証明書である新サーバ証明書を前記サーバ装置に送信する第４の手順とを適当な順番で実行し、
このとき、前記第２の手順と前記第３の手順とを一括して実行し、これらの手順の完了後、前記クライアントから前記新証明鍵を受信した旨の情報を受信した後で、前記第１の手順と前記第４の手順とを一括して実行するようにしたことを特徴とするデジタル証明書管理方法。
【請求項２４】
前記デジタル証明書管理装置と前記クライアントとは前記サーバを介して通信を行い、
該サーバが、前記デジタル証明書管理装置が前記第２及び／又は第３の手順で前記クライアントに対して送信する新証明鍵及び／又は新クライアント証明書を、前記クライアントとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で前記クライアントに送信するようにしたことを特徴とする請求項１８乃至２３のいずれか一項記載のデジタル証明書管理方法。
【請求項２５】
前記デジタル証明書管理装置と前記サーバとは前記クライアントを介して通信を行い、
該クライアントが、前記デジタル証明書管理装置が前記第１及び／又は第４の手順で前記サーバに対して送信する新証明鍵及び／又は新サーバ証明書を、前記サーバとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で前記サーバに送信するようにしたことを特徴とする請求項１８乃至２３のいずれか一項記載のデジタル証明書管理方法。
【請求項２６】
請求項１８乃至２５のいずれか一項記載のデジタル証明書管理方法であって、
前記クライアントと前記サーバとの間の前記認証は、ＳＳＬ又はＴＬＳのプロトコルに従った認証であり、
前記サーバ証明書は前記サーバの公開鍵証明書であることを特徴とするデジタル証明書管理方法。
【請求項２７】
クライアント・サーバシステムを構成するクライアント及びサーバと通信可能なデジタル証明書管理装置を制御するコンピュータに、
前記クライアントと前記サーバとの間で通信を確立する際の認証に前記サーバが使用するデジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手順を実行させるためのプログラムであって、
前記コンピュータを、
更新用の新証明鍵を取得する手段と、
該新証明鍵を用いて正当性を確認可能な、前記認証に使用するための新デジタル証明書を取得する手段と、
前記新証明鍵を前記クライアントに送信する第１の送信手段と、
前記サーバのための新デジタル証明書である新サーバ証明書を前記サーバに送信する第２の送信手段として機能させるためのプログラムを含み、
該第２の送信手段が、前記サーバに対して前記新サーバ証明書を送信する動作を、前記クライアントから前記新証明鍵を受信した旨の情報を受信した後に行うようにしたことを特徴とするプログラム。
【請求項２８】
請求項２７記載のプログラムであって、
前記コンピュータを、従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって前記新証明鍵を含む証明鍵証明書を取得する手段として機能させるためのプログラムをさらに含み、
前記第１の送信手段が、前記新証明鍵を前記証明鍵証明書の形式で前記クライアントに送信するようにしたことを特徴とするプログラム。
【請求項２９】

請求項２７記載のプログラムであって、
前記コンピュータを、
従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって前記新証明鍵を含む第１の証明鍵証明書を取得する手段と、
前記新証明鍵を用いて正当性を確認可能なデジタル証明書であって前記新証明鍵を含む第２の証明鍵証明書を取得する手段として機能させるためのプログラムをさらに含み、
前記第１の送信手段が、前記新証明鍵を前記第１及び第２の証明鍵証明書の形式でそれぞれ前記クライアントに送信し、前記クライアントに、前記第２の証明鍵証明書を記憶する場合には従前の証明鍵証明書及び前記第１の証明鍵証明書を削除させる機能を有し、さらに、前記第２の証明鍵証明書を前記クライアントに送信する動作を、少なくとも前記サーバから前記新サーバ証明書を受信した旨の情報を受信した後に行う機能を有することを特徴とするプログラム。
【請求項３０】
クライアント・サーバシステムを構成するクライアント及びサーバと通信可能なデジタル証明書管理装置を制御するコンピュータに、
前記クライアントと前記サーバとの間で通信を確立する際の相互認証に使用するデジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手順を実行させるためのプログラムであって、
前記コンピュータを、
更新用の新証明鍵を取得する手段と、
該新証明鍵を用いて正当性を確認可能な、前記相互認証に使用するための新デジタル証明書を取得する手段と、
前記クライアントのための新デジタル証明書である新クライアント証明書と、前記新証明鍵とをそれぞれ前記クライアントに送信する第１の送信手段と、
前記サーバのための新デジタル証明書である新サーバ証明書と、前記新証明鍵とをそれぞれ前記サーバに送信する第２の送信手段として機能させるためのプログラムを含み、
該第２の送信手段が、前記サーバに対して前記新サーバ証明書を送信する動作を、前記クライアントから前記新証明鍵を受信した旨の情報を受信した後に行うようにし、
前記第１の送信手段が、前記クライアントに前記新クライアント証明書を送信する動作を、前記サーバから前記新証明鍵を受信した旨の情報を受信した後に行うようにしたことを特徴とするプログラム。
【請求項３１】
クライアント・サーバシステムを構成するクライアント及びサーバと通信可能なデジタル証明書管理装置を制御するコンピュータに、
前記クライアントと前記サーバとの間で通信を確立する際の相互認証に使用するデジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手順を実行させるためのプログラムであって、
前記コンピュータを、
更新用の新証明鍵を取得する手段と、
該新証明鍵を用いて正当性を確認可能な、前記相互認証に使用するための新デジタル証明書を取得する手段と、
前記クライアントのための新デジタル証明書である新クライアント証明書と、前記新証明鍵とをそれぞれ前記クライアントに送信する第１の送信手段と、
前記サーバのための新デジタル証明書である新サーバ証明書と、前記新証明鍵とをそれぞれ前記サーバに送信する第２の送信手段として機能させるためのプログラムを含み、
前記第１の送信手段の機能が、前記新クライアント証明書と前記新証明鍵とを同時に前記クライアントに送信する機能であり、
前記第２の送信手段の機能が、前記クライアントから前記新証明鍵を受信した旨の情報を受信した後で、前記新サーバ証明書と前記新証明鍵とを同時に前記サーバに送信する機能であることを特徴とするプログラム。

【請求項３２】
前記コンピュータを、前記クライアントとは前記サーバを介して通信を行うよう機能させるためのプログラムを含み、
該サーバは、前記第１の送信手段が前記クライアントに対して送信する新証明鍵及び／又は新クライアント証明書を、前記クライアントとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で前記クライアントに送信するサーバであることを特徴とする請求項２７乃至３１のいずれか一項記載のプログラム。
【請求項３３】
前記コンピュータを、前記サーバとは前記クライアントを介して通信を行うよう機能させるためのプログラムを含み、
該クライアントは、前記第２の送信手段が前記サーバに対して送信する新証明鍵及び／又は新サーバ証明書を、前記サーバとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で前記サーバに送信するクライアントであることを特徴とする請求項２７乃至３１のいずれか一項記載のプログラム。
【請求項３４】
請求項２７乃至３３のいずれか一項記載のプログラムであって、
前記認証は、ＳＳＬ又はＴＬＳのプロトコルに従った認証であり、
前記サーバ証明書は前記サーバの公開鍵証明書であることを特徴とするプログラム。

【書類名】明細書
【発明の名称】デジタル証明書管理システム、デジタル証明書管理装置、デジタル証明書管理方法およびプログラム
【技術分野】
【０００１】
この発明は、デジタル証明書管理装置によってクライアント・サーバシステムを構成するクライアントとサーバの間の認証処理に用いるデジタル証明書を管理するデジタル証明書管理システム、このようなシステムを構成するデジタル証明書管理装置、このようにデジタル証明書を管理するデジタル証明書管理方法、およびコンピュータを上記のデジタル証明書管理装置として機能させるためのプログラムに関する。
【背景技術】
【０００２】
従来から、ＰＣ等のコンピュータを複数台ネットワークを介して通信可能に接続し、少なくとも１台をサーバ装置（サーバ）、別の少なくとも１台をクライアント装置（クライアント）としたクライアント・サーバシステムを構成することが行われている。
このようなクライアント・サーバシステムにおいては、クライアント装置からサーバ装置に要求を送信し、サーバ装置がその要求に従った処理を行ってクライアント装置に対して応答を返す。そして、このようなクライアント・サーバシステムは、クライアント装置から商品の注文要求を送信し、サーバ装置においてその注文を受け付けるといった、いわゆる電子商取引にも広く用いられるようになっている。また、種々の電子装置にクライアント装置あるいはサーバ装置の機能を持たせてネットワークを介して接続し、相互間の通信によって電子装置の遠隔管理を行うシステムも提案されている。
【０００３】
このような場合においては、通信相手が適切か、あるいは送信される情報が改竄されていないかといった確認が重要である。また、特にインターネットにおいては、情報が通信相手に到達するまでに無関係なコンピュータを経由する場合が多いことから、機密情報を送信する場合、その内容を盗み見られないようにする必要もある。そして、このような要求に応える通信プロトコルとして、例えばＳＳＬ（Secure Socket Layer）と呼ばれるプロトコルが開発されており、広く用いられている。このプロトコルを用いて通信を行うことにより、公開鍵暗号方式と共通鍵暗号方式とを組み合わせ、通信相手の認証を行うと共に、情報の暗号化により改竄及び盗聴の防止を図ることができる。
【０００４】
ここで、公開鍵暗号方式を用いて認証処理を行う場合の通信手順及びその際に使用するデジタル証明書について説明する。なおここでは、クライアント装置がサーバ装置を認証する場合を例として説明する。
この場合、認証処理を行うために、サーバ装置側にサーバ私有鍵及びサーバ公開鍵証明書（サーバ証明書）を記憶させると共に、クライアント装置側にルート鍵証明書を記憶させておく。ここで、サーバ私有鍵は、認証局（ＣＡ：certificate authority）がサーバ装置に対して発行した私有鍵である。そして、サーバ公開鍵証明書は、その私有鍵と対応する公開鍵にＣＡがデジタル署名を付してデジタル証明書としたものである。また、ルート鍵証明書は、ＣＡがデジタル署名に用いた証明用私有鍵であるルート私有鍵と対応する証明用公開鍵（以下「証明鍵」ともいう）であるルート鍵に、デジタル署名を付してデジタル証明書としたものである。
【０００５】
図４１にこれらの関係を示す。
図４１（ａ）に示すように、サーバ公開鍵は、サーバ私有鍵を用いて暗号化された文書を復号化するための鍵本体と、その公開鍵の発行者（ＣＡ），発行相手（サーバ装置），有効期限等の情報を含む書誌情報とによって構成される。そして、ＣＡは、鍵本体や書誌情報が改竄されていないことを示すため、サーバ公開鍵をハッシュ処理して得たハッシュ値を、ルート私有鍵を用いて暗号化し、デジタル署名としてサーバ公開鍵に付す。またこ

の際に、デジタル署名に用いるルート私有鍵の識別情報を署名鍵情報として公開鍵の書誌情報に加える。そして、このデジタル署名を付した公開鍵証明書が、サーバ公開鍵証明書である。

【０００６】

このサーバ公開鍵証明書を認証処理に用いる場合には、ここに含まれるデジタル署名を、ルート私有鍵と対応する公開鍵であるルート鍵の鍵本体を用いて復号化する。この復号化が正常に行われれば、デジタル署名が確かにＣＡによって付されたことがわかる。また、サーバ公開鍵部分をハッシュ処理して得たハッシュ値と、復号して得たハッシュ値とが一致すれば、鍵自体も損傷や改竄を受けていないことがわかる。さらに、受信したデータをこのサーバ公開鍵を用いて正常に復号化できれば、そのデータは、サーバ私有鍵の持ち主、つまりサーバ装置から送信されたものであることがわかる。あとは、書誌情報を参照して、ＣＡの信頼性やサーバ装置の登録有無等によって認証の正否を決定すればよい。

【０００７】

ここで、認証を行うためには、ルート鍵を予め記憶しておく必要があるが、このルート鍵も、図４１（ｂ）に示すように、ＣＡがデジタル署名を付したルート鍵証明書として記憶しておく。このルート鍵証明書は、自身に含まれる公開鍵でデジタル署名を復号化可能な、自己署名形式である。そして、ルート鍵を使用する際に、そのルート鍵証明書に含まれる鍵本体を用いてデジタル署名を復号化し、ルート鍵をハッシュ処理して得たハッシュ値と比較する。これが一致すれば、ルート鍵が破損等していないことを確認できるのである。

【０００８】

そして、以上のようなクライアント装置とサーバ装置とによって構成されるクライアント・サーバシステムにおいてクライアント装置がサーバ装置に通信を要求する場合、これらの各装置はそれぞれ以下のような処理を行う。

まずサーバ装置は、クライアント装置からの通信要求に応じて乱数を生成すると共に、これをサーバ私有鍵で暗号化し、その暗号化した乱数をサーバ公開鍵証明書と共にクライアント装置に送信する。

すると、これを受信したクライアント装置は、受信したサーバ公開鍵証明書の正当性をルート鍵証明書を用いて確認する。これには、上述のように損傷や改竄を受けていないことを確認するのみならず、書誌情報を参照してサーバ装置が適当な通信相手であることを確認する処理を含む。

【０００９】

そして確認ができると、受信したサーバ公開鍵証明書に含まれるサーバ公開鍵を用いて受信した乱数を復号化する。ここで復号化が成功すれば、第１の乱数は確かにサーバ公開鍵証明書の発行対象であるサーバ装置から受信したものだと確認できる。従って、以上の処理により、サーバ装置を正当な通信相手として認証することができる。

また、上記の公開鍵や私有鍵で暗号化して共通鍵暗号の鍵を交換するようにすれば、安全に共通鍵を交換し、通信内容を共通鍵暗号によって暗号化した安全な通信経路を確立することができる。

【００１０】

ところで、公開鍵暗号方式においては、鍵長にもよるが、時間をかければ公開鍵から私有鍵を導くことができる。そして、私有鍵がわかってしまえば、第３者がその私有鍵の持ち主になりすますことが可能になるので、認証の確実性や通信の安全性が保たれない。そこで、上述のように鍵に有効期限を設け、所定期間毎に鍵のセットを更新するというセキュリティポリシーを採用するユーザが増えている。このため、例えば上記のような認証処理を利用した遠隔管理システム等を提供する場合には、顧客に対し、鍵の更新が可能なシステムであるという保証を行う必要が生じている。これは、ルート鍵とルート私有鍵についても同様である。なお、鍵の更新事由としては、所定の有効期限の到来の他にも、私有鍵の第３者への漏洩が判明した場合等が考えられる。

このような鍵の更新に関する技術としては、例えば特許文献１に記載のものが挙げられ

る。

【特許文献１】特開平１１－１２２２３８号公報

【発明の開示】

【発明が解決しようとする課題】

【００１１】

しかしながら、特許文献１には、各装置に対して発行した鍵の更新に関する記載はあるが、ルート鍵の更新についての記載はない。

公開鍵暗号方式の場合、各装置に発行した鍵のペアを更新する場合には、その装置には新たな私有鍵に対応した新たな公開鍵証明書が記憶されることになり、通信相手にこれを渡せば、上述のような認証処理を支障なく行うことができる。

しかし、ルート鍵を更新する場合、新たなルート鍵では従前のデジタル証明書に付されたデジタル署名を復号化することができないため、新たなルート鍵と対応する新たなルート私有鍵を用いて各装置の公開鍵証明書を作成し直し、これを配布しなければ、認証処理の実行に支障を来してしまう（ただし、各装置の私有鍵は必ずしも更新する必要はない）。

【００１２】

そして、認証処理に支障を来さずにこのようなルート鍵を更新する方式が知られていなかったため、更新の必要な装置にルート鍵をネットワークを介して安全に送信することができなかった。そこで、ルート鍵証明書や新たな公開鍵証明書を別の安全な経路で各装置に届ける必要があった。すなわち、ルート鍵更新用の特別な通信経路を設ける必要があったのである。

この経路としては、例えば書留郵便が考えられ、証明書のデータを記録したメモリカードやフレキシブルディスク等の記録媒体を装置の管理者に書留郵便で送付し、管理者が装置の鍵を更新するという方式が考えられる。しかし、この方式では、クライアントやサーバの各装置について十分な知識を持った管理者がいる場合にしか適用できないし、ＣＡ側は記録媒体を送付した後の処理については装置の管理者を信用するしかなかった。従って、管理者が更新処理を怠ったり誤ったりした場合には、認証処理が行えなくなってしまうという問題があった。

【００１３】

一方管理者側も、受け取った証明書が正しいものであるか否かは、封筒やデータに記載された送り主の名称等を信用して判断するしかなく、ＣＡの名を騙る別人から受け取ったニセの証明書を装置に記憶させてしまうといった危険は常につきまとうことになる。

また、ＣＡやクライアント・サーバシステムによるサービスの提供者が、各装置の配置先にサービスマンを派遣して鍵の更新を行うことも考えられるが、広い地域でこのような方式を採るには多数のサービス拠点が必要になり、コストが嵩むことになる。また、サービスマンの教育や不正防止、更新作業用の管理者ＩＤの管理も問題となる。例えば、認証情報を手入力する単純な方式を採ろうとすると、退職したサービスマンについての更新権限を抹消するためには、各装置に記憶させている認証情報を変更する必要があるが、顧客先に設置された多数の装置にこのような変更を行うことは困難である。

【００１４】

結局のところ、ネットワークを介さずに証明書の安全な配布経路を確保するためには、人間を信用する他なく、そこには欺瞞が入りこむ余地が出てしまう。そして、この余地を小さくするよう管理することはできるが、そのためには膨大なコストが生じてしまい、欺瞞の危険を考慮しなくて済むレベルの経路を証明書の配布のために構築することは、現実的ではなかった。

【００１５】

また、更新用の特別な通信経路としては、通常の通信に使用するデジタル証明書及びルート鍵証明書とは別の、更新処理用デジタル証明書及び更新処理用ルート鍵証明書を用いた通信経路を用意することも考えられる。しかしながら、クライアント装置がサーバ装置を認証するシステムの場合、このような手法には問題がある。

すなわち、この場合サーバ装置は、クライアント装置から接続要求があった場合にデジタル証明書をクライアント装置に送信するのであるが、不特定多数のクライアント装置から任意のタイミングで接続要求を受け得るサーバ装置の場合、通常通信用と更新処理用のいずれのデジタル証明書をクライアント装置に送信すればよいかを適切に判断することは困難である。

【００１６】

仮に判断しようとすれば、例えば通信要求の際のソースエンドポイントアイデンティファイア、デスティネーションエンドポイントアイデンティファイアやＵＲＬ（Uniform Resource Locator）のようなセッション識別子を利用して判断することが考えられる。しかしながら、このような判断を行うためには、クライアント装置側に通常通信か更新用通信かに応じてセッション識別子（例えばＵＲＬ）を切換える機能を設けたり、サーバ装置側にソースエンドポイントアイデンティファイアと送信すべきデジタル証明書との対応関係を管理する機能を設けたりする必要が生じる。そして、このような機能を設けることは、コストアップにつながる。

【００１７】

従って、サーバ装置に、セッション識別子のような通信開始前の情報に基づいてクライアント装置に送信すべきデジタル証明書を選択する機能を設けることは避けたいという要求があった。また、同じプロトコルを利用して２種の通信経路を設けると、認証が失敗した場合に、それがデジタル証明書の異常によるものか、セッション識別子の誤りによるものかを区別し難いという問題も生じる。

以上のように、ルート鍵更新用の特別な通信経路を設けることは、コストや管理の負担を増すことになるので、このような特別な通信経路を設けることなく、ルート鍵を安全に更新したいという要求があった。

【００１８】

この発明は、このような問題を解決し、クライアント・サーバシステムにおける認証処理でデジタル証明書の正当性を確認するために用いる証明鍵を、更新用の特別な通信経路を設けることなく安全に更新できるようにすることを目的とする。

【課題を解決するための手段】

【００１９】

上記の目的を達成するため、この発明のデジタル証明書管理システムは、クライアントとサーバとの間で通信を確立する際にデジタル証明書を用いて認証を行い、その認証に伴って確立した通信経路で通信を行うようにしたクライアント・サーバシステムと、上記クライアント及び上記サーバと通信可能なデジタル証明書管理装置とを備えた証明書管理システムにおいて、上記デジタル証明書管理装置に、上記サーバが上記認証に使用する上記デジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手段を設け、その証明鍵更新手段に、更新用の新証明鍵を取得する手段と、その新証明鍵を用いて正当性を確認可能な、上記認証に使用するための新デジタル証明書を取得する手段と、上記新証明鍵を上記クライアントに送信する第１の送信手段と、上記サーバのための新デジタル証明書である新サーバ証明書を上記サーバに送信する第２の送信手段とを設け、その第２の送信手段を、上記サーバに対して上記新サーバ証明書を送信する動作を、上記クライアントから上記新証明鍵を受信した旨の情報を受信した後に行う手段としたものである。

【００２０】

このようなデジタル証明書管理システムにおいて、上記デジタル証明書管理装置の上記証明鍵更新手段に、従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって上記新証明鍵を含む証明鍵証明書を取得する手段を設け、上記第１の送信手段を、上記新証明鍵を上記証明鍵証明書の形式で上記クライアントに送信する手段とし、上記クライアントに、上記デジタル証明書管理装置から上記証明鍵証明書に含まれる証明鍵を受信した場合に、受信した証明鍵証明書の正当性を従前の証明鍵を用いて確認し、そこに含まれる証明鍵が適当なものであると判断した場合にその証明鍵を記憶する手段を設けるとよい。

【００２１】

あるいは、上記デジタル証明書管理装置の上記証明鍵更新手段に、従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって上記新証明鍵を含む第１の証明鍵証明書を取得する手段と、上記新証明鍵を用いて正当性を確認可能なデジタル証明書であって上記新証明鍵を含む第２の証明鍵証明書を取得する手段とを設け、上記第１の送信手段を、上記新証明鍵を上記第１及び第２の証明鍵証明書の形式でそれぞれ上記クライアントに送信する手段とし、上記クライアントに、上記デジタル証明書管理装置から上記第１の証明鍵証明書を受信した場合に、その証明書の正当性を従前の証明鍵を用いて確認し、これが適当なものであると判断した場合にその証明書を記憶する手段と、上記デジタル証明書管理装置から上記第２の証明鍵証明書を受信した場合に、その証明書の正当性を上記第１の証明鍵証明書に含まれる上記新証明鍵を用いて確認し、上記第２の証明鍵証明書が適当なものであると判断した場合に、その証明書を記憶すると共に従前の証明鍵証明書及び上記第１の証明鍵証明書を削除する手段とを設け、上記デジタル証明書管理装置の上記第１の送信手段を、上記第２の証明鍵証明書を上記クライアントに送信する動作を、少なくとも上記サーバから上記新サーバ証明書を受信した旨の情報を受信した後に行う手段としてもよい。

【００２２】

また、この発明は、クライアントとサーバとの間で通信を確立する際にデジタル証明書を用いて相互認証を行い、その認証に伴って確立した通信経路で通信を行うようにしたクライアント・サーバシステムと、上記クライアント及び上記サーバと通信可能なデジタル証明書管理装置とを備えた証明書管理システムにおいて、上記デジタル証明書管理装置に、上記クライアント及び上記サーバが上記相互認証に使用する上記デジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手段を設け、その証明鍵更新手段に、更新用の新証明鍵を取得する手段と、その新証明鍵を用いて正当性を確認可能な、上記相互認証に使用するための新デジタル証明書を取得する手段と、上記クライアントのための新デジタル証明書である新クライアント証明書と、上記新証明鍵とをそれぞれ上記クライアントに送信する第１の送信手段と、上記サーバのための新デジタル証明書である新サーバ証明書と、上記新証明鍵とをそれぞれ上記サーバに送信する第２の送信手段とを設け、その第２の送信手段を、上記サーバに対して上記新サーバ証明書を送信する動作を、上記クライアントから上記新証明鍵を受信した旨の情報を受信した後に行う手段とし、上記第１の送信手段を、上記クライアントに上記新クライアント証明書を送信する動作を、上記サーバから上記新証明鍵を受信した旨の情報を受信した後に行う手段としたデジタル証明書管理システムも提供する。

このような証明書管理システムにおいて、上記第１の送信手段を、上記新証明鍵を、上記新クライアント証明書と同時あるいはそれより前に上記クライアントに送信する手段とし、上記第２の送信手段を、上記新証明鍵を、上記新サーバ証明書と同時あるいはそれより前に上記サーバに送信する手段とするとよい。

【００２３】

また、この発明は、クライアントとサーバとの間で通信を確立する際にデジタル証明書を用いて相互認証を行い、その認証に伴って確立した通信経路で通信を行うようにしたクライアント・サーバシステムと、上記クライアント及び上記サーバと通信可能なデジタル証明書管理装置とを備えた証明書管理システムにおいて、上記デジタル証明書管理装置に、上記クライアント及び上記サーバが上記相互認証に使用する上記デジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手段を設け、その証明鍵更新手段に、更新用の新証明鍵を取得する手段と、その新証明鍵を用いて正当性を確認可能な、上記相互認証に使用するための新デジタル証明書を取得する手段と、上記クライアントのための新デジタル証明書である新クライアント証明書と、上記新証明鍵とをそれぞれ上記クライアントに送信する第１の送信手段と、上記サーバのための新デジタル証明書である新サーバ証明書と、上記新証明鍵とをそれぞれ上記サーバに送信する第２の送信手段とを設け、上記第１の送信手段を、上記新クライアント証明書と上記新証明鍵とを同時に上記クライアントに送信する手段とし、上記第２の送信手段を、上記クライアントから上記新証明鍵を

受信した旨の情報を受信した後で、上記新サーバ証明書と上記新証明鍵とを同時に上記サーバに送信する手段としたデジタル証明書管理システムも提供する。

【００２４】

上記の各デジタル証明書管理システムにおいて、上記サーバに、上記デジタル証明書管理装置と上記クライアントとの間の通信を仲介する手段を設け、上記デジタル証明書管理装置と上記クライアントとは上記サーバを介して通信を行い、そのサーバが、上記デジタル証明書管理装置の第１の送信手段が上記クライアントに対して送信する新証明鍵及び／又は新クライアント証明書を、上記クライアントとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で上記クライアントに送信するようにするとよい。

あるいは、上記クライアントに、上記デジタル証明書管理装置と上記サーバとの間の通信を仲介する手段を設け、上記デジタル証明書管理装置と上記サーバとは上記クライアントを介して通信を行い、そのクライアントが、上記デジタル証明書管理装置の第２の送信手段が上記サーバに対して送信する新証明鍵及び／又は新サーバ証明書を、上記サーバとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で上記サーバに送信するようにしてもよい。

さらに、上記クライアントと上記サーバが行う認証を、ＳＳＬ又はＴＬＳのプロトコルに従った認証とし、上記サーバ証明書を上記サーバの公開鍵証明書とするとよい。

【００２５】

また、この発明のデジタル証明書管理装置は、クライアント・サーバシステムを構成するクライアント及びサーバと通信可能なデジタル証明書管理装置において、上記クライアントと上記サーバとの間で通信を確立する際の認証に使用するデジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手段を設け、その証明鍵更新手段に、更新用の新証明鍵を取得する手段と、その新証明鍵を用いて正当性を確認可能な、上記認証に使用するための新デジタル証明書を取得する手段と、上記新証明鍵を上記クライアントに送信する第１の送信手段と、上記サーバのための新デジタル証明書である新サーバ証明書を上記サーバに送信する第２の送信手段とを設け、その第２の送信手段を、上記サーバに対して上記新サーバ証明書を送信する動作を、上記クライアントから上記新証明鍵を受信した旨の情報を受信した後に行う手段とするとよい。

【００２６】

このようなデジタル証明書管理装置において、上記証明鍵更新手段に、従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって上記新証明鍵を含む証明鍵証明書を取得する手段を設け、上記第１の送信手段を、上記新証明鍵を上記証明鍵証明書の形式で上記クライアントに送信してここに含まれる証明鍵を記憶するよう要求する手段とするとよい。

【００２７】

あるいは、上記証明鍵更新手段に、従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって上記新証明鍵を含む第１の証明鍵証明書を取得する手段と、上記新証明鍵を用いて正当性を確認可能なデジタル証明書であって上記新証明鍵を含む第２の証明鍵証明書を取得する手段とを設け、上記第１の送信手段を、上記新証明鍵を上記第１及び第２の証明鍵証明書の形式でそれぞれ上記クライアントに送信する手段とし、上記クライアントに、上記第２の証明鍵証明書を記憶する場合には従前の証明鍵証明書及び上記第１の証明鍵証明書を削除させる手段を設け、上記第２の証明鍵証明書を上記クライアントに送信する動作を、少なくとも上記サーバから上記新サーバ証明書を受信した旨の情報を受信した後に行うようにするようにするとよい。

【００２８】

また、この発明は、クライアント・サーバシステムを構成するクライアント及びサーバと通信可能なデジタル証明書管理装置において、上記クライアントと上記サーバとの間で通信を確立する際の相互認証に上記サーバが使用するデジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手段を設け、その証明鍵更新手段に、更新用の新証明

鍵を取得する手段と、その新証明鍵を用いて正当性を確認可能な、上記相互認証に使用するための新デジタル証明書を取得する手段と、上記クライアントのための新デジタル証明書である新クライアント証明書と、上記新証明鍵とをそれぞれ上記クライアントに送信する第１の送信手段と、上記サーバのための新デジタル証明書である新サーバ証明書と、上記新証明鍵とをそれぞれ上記サーバに送信する第２の送信手段とを設け、その第２の送信手段を、上記サーバに対して上記新サーバ証明書を送信する動作を、上記クライアントから上記新証明鍵を受信した旨の情報を受信した後に行う手段とし、上記第１の送信手段を、上記クライアントに上記新クライアント証明書を送信する動作を、上記サーバから上記新証明鍵を受信した旨の情報を受信した後に行う手段としたデジタル証明書管理装置も提供する。

【００２９】

さらにまた、クライアント・サーバシステムを構成するクライアント及びサーバと通信可能なデジタル証明書管理装置において、上記クライアントと上記サーバとの間で通信を確立する際の相互認証に使用するデジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手段を設け、その証明鍵更新手段に、更新用の新証明鍵を取得する手段と、その新証明鍵を用いて正当性を確認可能な、上記相互認証に使用するための新デジタル証明書を取得する手段と、上記クライアントのための新デジタル証明書である新クライアント証明書と、上記新証明鍵とをそれぞれ上記クライアントに送信する第１の送信手段と、上記サーバのための新デジタル証明書である新サーバ証明書と、上記新証明鍵とをそれぞれ上記サーバに送信する第２の送信手段とを設け、上記第１の送信手段を、上記新クライアント証明書と上記新証明鍵とを同時に上記クライアントに送信する手段とし、上記第２の送信手段が、上記クライアントから上記新証明鍵を受信した旨の情報を受信した後で、上記新サーバ証明書と上記新証明鍵とを同時に上記サーバに送信する手段としたデジタル証明書管理装置も提供する。

【００３０】

また、これらのデジタル証明書管理装置において、上記クライアントとは上記サーバを介して通信を行うようにし、そのサーバを、上記第１の送信手段が上記クライアントに対して送信する新証明鍵及び／又は新クライアント証明書を、上記クライアントとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で上記クライアントに送信するサーバとするとよい。

あるいは、上記サーバとは上記クライアントを介して通信を行うようにし、そのクライアントを、上記第２の送信手段が上記サーバに対して送信する新証明鍵及び／又は新サーバ証明書を、上記サーバとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で上記サーバに送信するクライアントとするとよい。

また、上記の各デジタル証明書管理装置において、上記認証を、ＳＳＬ又はＴＬＳのプロトコルに従った認証とし、上記サーバ証明書を上記サーバの公開鍵証明書とするとよい。

【００３１】

また、この発明のデジタル証明書管理方法は、クライアント・サーバシステムを構成するクライアントとサーバとの間で通信を確立する際の認証に使用するデジタル証明書を、上記クライアント及び上記サーバと通信可能なデジタル証明書管理装置によって管理するデジタル証明書管理方法において、上記デジタル証明書管理装置が、上記サーバが上記認証に使用する上記デジタル証明書の正当性を確認するための証明鍵を更新し、その証明鍵の更新を、更新用の新証明鍵を取得する手順と、その新証明鍵を用いて正当性を確認可能な、上記認証に使用するための新デジタル証明書を取得する手順とを実行し、さらに、上記新証明鍵を上記クライアントに送信する第１の手順を実行した後、そのクライアントからその新証明鍵を受信した旨の情報を受信した後で、上記サーバのための新デジタル証明書である新サーバ証明書を上記サーバ装置に送信する第２の手順を実行するようにしたものである。

【００３２】

このようなデジタル証明書管理方法において、上記証明鍵の更新の際に、従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって上記新証明鍵を含む証明鍵証明書を取得する手順をさらに実行し、上記第１の手順を、上記新証明鍵を上記証明鍵証明書の形式で上記クライアントに送信する手順とし、上記クライアントに上記証明鍵証明書を送信する場合に、その証明鍵証明書の正当性を記憶している従前の証明鍵を用いて確認させ、そこに含まれる証明鍵が適当なものであると判断した場合にその証明鍵を記憶させるようにするとよい。

【００３３】

あるいは、上記証明鍵の更新の際に、従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって上記新証明鍵を含む第１の証明鍵証明書を取得する手順と、上記新証明鍵を用いて正当性を確認可能なデジタル証明書であって上記新証明鍵を含む第２の証明鍵証明書を取得する手順とをさらに実行し、上記第１の手順において、上記新証明鍵を上記第１の証明鍵証明書の形式で上記クライアントに送信し、上記第２の手順の完了後、少なくとも上記サーバから上記新サーバ証明書を受信した旨の情報を受信した後に、上記第２の証明鍵証明書を上記クライアントに送信する手順を実行し、上記クライアントに上記第１の証明鍵証明書を送信する際に、その証明書の正当性を従前の証明鍵を用いて確認させ、これが適当なものであると判断した場合にその証明書を記憶させ、上記クライアントに上記第２の証明鍵証明書を送信する際に、その証明書の正当性を上記第１の証明鍵証明書に含まれる上記新証明鍵を用いて確認させ、上記第２の証明鍵証明書が適当なものであると判断した場合に、その証明書を記憶させると共に従前の証明鍵証明書及び上記第１の証明鍵証明書を削除させるようにするとよい。

【００３４】

また、この発明は、クライアント・サーバシステムを構成するクライアントとサーバとの間で通信を確立する際の相互認証に使用するデジタル証明書を、上記クライアント及び上記サーバと通信可能なデジタル証明書管理装置によって管理するデジタル証明書管理方法において、上記デジタル証明書管理装置が、上記クライアント及び上記サーバが上記相互認証に使用する上記デジタル証明書の正当性を確認するための証明鍵を更新し、その証明鍵の更新を、更新用の新証明鍵を取得する手順と、その新証明鍵を用いて正当性を確認可能な、上記相互認証に使用するための新デジタル証明書を取得する手順とを実行し、さらに、上記新証明鍵を上記サーバに送信する第１の手順と、上記新証明鍵を上記クライアントに送信する第２の手順と、上記クライアントのための新デジタル証明書である新クライアント証明書を上記クライアントに送信する第３の手順と、上記サーバのための新デジタル証明書である新サーバ証明書を上記サーバ装置に送信する第４の手順とを適当な順番で実行し、このとき少なくとも、上記第４の手順を、上記第２の手順の完了後、上記クライアントから上記新証明鍵を受信した旨の情報を受信した後に、上記第３の手順を、上記第１の手順の完了後、上記サーバから上記新証明鍵を受信した旨の情報を受信した後に実行するようにしたデジタル証明書管理方法も提供する。

このようなデジタル証明書管理方法において、上記第３の手順を上記第２の手順と同時又はその完了後に、上記第４の手順を上記第１の手順と同時又はその完了後に実行するようにするとよい。

【００３５】

また、この発明は、クライアント・サーバシステムを構成するクライアントとサーバとの間で通信を確立する際の相互認証に使用するデジタル証明書を、上記クライアント及び上記サーバと通信可能なデジタル証明書管理装置によって管理するデジタル証明書管理方法において、上記デジタル証明書管理装置が、上記クライアント及び上記サーバが上記相互認証に使用する上記デジタル証明書の正当性を確認するための証明鍵を更新し、その証明鍵の更新を、更新用の新証明鍵を取得する手順と、その新証明鍵を用いて正当性を確認可能な、上記相互認証に使用するための新デジタル証明書を取得する手順とを実行し、さらに、上記新証明鍵を上記サーバに送信する第１の手順と、上記新証明鍵を上記クライアントに送信する第２の手順と、上記クライアントのための新デジタル証明書である新クラ

イアント証明書を上記クライアントに送信する第３の手順と、上記サーバのための新デジタル証明書である新サーバ証明書を上記サーバ装置に送信する第４の手順とを適当な順番で実行し、このとき、上記第２の手順と上記第３の手順とを一括して実行し、これらの手順の完了後、上記クライアントから上記新証明鍵を受信した旨の情報を受信した後で、上記第１の手順と上記第４の手順とを一括して実行するようにしたデジタル証明書管理方法も提供する。

【００３６】

また、上記の各デジタル証明書管理方法において、上記デジタル証明書管理装置と上記クライアントとが上記サーバを介して通信を行い、そのサーバが、上記デジタル証明書管理装置が上記第２及び／又は第３の手順で上記クライアントに対して送信する新証明鍵及び／又は新クライアント証明書を、上記クライアントとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で上記クライアントに送信するようにするとよい。

あるいは、上記デジタル証明書管理装置と上記サーバとが上記クライアントを介して通信を行い、そのクライアントが、上記デジタル証明書管理装置が上記第１及び／又は第４の手順で上記サーバに対して送信する新証明鍵及び／又は新サーバ証明書を、上記サーバとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で上記サーバに送信するようにするとよい。

さらに、以上の各デジタル証明書管理方法において、上記クライアントと上記サーバとの間の上記認証を、ＳＳＬ又はＴＬＳのプロトコルに従った認証とし、上記サーバ証明書を上記サーバの公開鍵証明書とするとよい。

【００３７】

また、この発明のプログラムは、クライアント・サーバシステムを構成するクライアント及びサーバと通信可能なデジタル証明書管理装置を制御するコンピュータに、上記クライアントと上記サーバとの間で通信を確立する際の認証に上記サーバが使用するデジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手順を実行させるためのプログラムにおいて、上記コンピュータを、更新用の新証明鍵を取得する手段と、その新証明鍵を用いて正当性を確認可能な、上記認証に使用するための新デジタル証明書を取得する手段と、上記新証明鍵を上記クライアントに送信する第１の送信手段と、上記サーバのための新デジタル証明書である新サーバ証明書を上記サーバに送信する第２の送信手段として機能させるためのプログラムを含め、その第２の送信手段が、上記サーバに対して上記新サーバ証明書を送信する動作を、上記クライアントから上記新証明鍵を受信した旨の情報を受信した後に行うようにしたものである。

【００３８】

このようなプログラムにおいて、上記コンピュータを、従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって上記新証明鍵を含む証明鍵証明書を取得する手段として機能させるためのプログラムをさらに含め、上記第１の送信手段が、上記新証明鍵を上記証明鍵証明書の形式で上記クライアントに送信するようにするとよい。

【００３９】

あるいは、上記コンピュータを、従前の証明鍵を用いて正当性を確認可能なデジタル証明書であって上記新証明鍵を含む第１の証明鍵証明書を取得する手段と、上記新証明鍵を用いて正当性を確認可能なデジタル証明書であって上記新証明鍵を含む第２の証明鍵証明書を取得する手段として機能させるためのプログラムをさらに含め、上記第１の送信手段に、上記新証明鍵を上記第１及び第２の証明鍵証明書の形式でそれぞれ上記クライアントに送信し、上記クライアントに、上記第２の証明鍵証明書を記憶する場合には従前の証明鍵証明書及び上記第１の証明鍵証明書を削除させる機能を設け、さらに、上記第２の証明鍵証明書を上記クライアントに送信する動作を、少なくとも上記サーバから上記新サーバ証明書を受信した旨の情報を受信した後に行う機能を設けるとよい。

【００４０】

また、この発明は、クライアント・サーバシステムを構成するクライアント及びサーバ

と通信可能なデジタル証明書管理装置を制御するコンピュータに、上記クライアントと上記サーバとの間で通信を確立する際の相互認証に使用するデジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手順を実行させるためのプログラムにおいて、上記コンピュータを、更新用の新証明鍵を取得する手段と、その新証明鍵を用いて正当性を確認可能な、上記相互認証に使用するための新デジタル証明書を取得する手段と、上記クライアントのための新デジタル証明書である新クライアント証明書と、上記新証明鍵とをそれぞれ上記クライアントに送信する第１の送信手段と、上記サーバのための新デジタル証明書である新サーバ証明書と、上記新証明鍵とをそれぞれ上記サーバに送信する第２の送信手段として機能させるためのプログラムを含め、その第２の送信手段が、上記サーバに対して上記新サーバ証明書を送信する動作を、上記クライアントから上記新証明鍵を受信した旨の情報を受信した後に行うようにし、上記第１の送信手段が、上記クライアントに上記新クライアント証明書を送信する動作を、上記サーバから上記新証明鍵を受信した旨の情報を受信した後に行うようにしたプログラムも提供する。

【００４１】

あるいはまた、この発明は、クライアント・サーバシステムを構成するクライアント及びサーバと通信可能なデジタル証明書管理装置を制御するコンピュータに、上記クライアントと上記サーバとの間で通信を確立する際の相互認証に使用するデジタル証明書の正当性を確認するための証明鍵を更新する証明鍵更新手順を実行させるためのプログラムにおいて、上記コンピュータを、更新用の新証明鍵を取得する手段と、その新証明鍵を用いて正当性を確認可能な、上記相互認証に使用するための新デジタル証明書を取得する手段と、上記クライアントのための新デジタル証明書である新クライアント証明書と、上記新証明鍵とをそれぞれ上記クライアントに送信する第１の送信手段と、上記サーバのための新デジタル証明書である新サーバ証明書と、上記新証明鍵とをそれぞれ上記サーバに送信する第２の送信手段として機能させるためのプログラムを含め、上記第１の送信手段の機能を、上記新クライアント証明書と上記新証明鍵とを同時に上記クライアントに送信する機能とし、上記第２の送信手段の機能を、上記クライアントから上記新証明鍵を受信した旨の情報を受信した後で、上記新サーバ証明書と上記新証明鍵とを同時に上記サーバに送信する機能としたプログラムも提供する。

【００４２】

また、これらのプログラムにおいて、上記コンピュータを、上記クライアントとは上記サーバを介して通信を行うよう機能させるためのプログラムを含め、そのサーバを、上記第１の送信手段が上記クライアントに対して送信する新証明鍵及び／又は新クライアント証明書を、上記クライアントとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で上記クライアントに送信するサーバとするとよい。

あるいは、上記コンピュータを、上記サーバとは上記クライアントを介して通信を行うよう機能させるためのプログラムを含め、そのクライアントを、上記第２の送信手段が上記サーバに対して送信する新証明鍵及び／又は新サーバ証明書を、上記サーバとの間で従前のデジタル証明書を用いた認証を行い、その認証に伴って確立した通信経路で上記サーバに送信するクライアントとするとよい。

さらに、以上の各プログラムにおいて、上記認証を、ＳＳＬ又はＴＬＳのプロトコルに従った認証とし、上記サーバ証明書を上記サーバの公開鍵証明書とするとよい。

【発明の効果】

【００４３】

以上のようなこの発明のデジタル証明書管理システム、デジタル証明書管理装置、デジタル証明書管理方法によれば、クライアント・サーバシステムにおける認証処理でデジタル証明書の正当性を確認するために用いる証明鍵を、更新用の特別な通信経路を設けることなく安全に更新できるようにすることができる。

また、この発明のプログラムによれば、コンピュータにデジタル証明書管理装置を制御させてこのようなデジタル証明書管理装置の特徴を実現し、同様な効果を得ることができる。

【発明を実施するための最良の形態】

【００４４】

以下、この発明の好ましい実施の形態を図面を参照して説明する。

〔第１の実施形態：図１乃至図１３〕

まず、この発明によるデジタル証明書管理装置である証明書管理装置と、クライアント・サーバシステムを構成するクライアント及びサーバによって構成される、この発明のデジタル証明書管理システムの第１の実施形態の構成について説明する。図２に、このデジタル証明書管理システムを構成する各装置の、この実施形態の特徴となる部分の機能構成を示す機能ブロック図を示す。図２において、この実施形態の特徴と関連しない部分の図示は省略している。

【００４５】

図２に示すように、このデジタル証明書管理システムは、証明書管理装置１０，サーバ装置３０，クライアント装置４０によって構成される。

そして、クライアント装置（クライアント）４０及びサーバ装置（サーバ）３０は、公開鍵暗号とデジタル証明書を用いる認証方式であるＳＳＬによる認証処理によって通信相手を正当な通信相手として認証した場合に、通信を確立させるようにしている。この認証が、互いが互いを認証する相互認証でも一方が他方を認証する片方向認証であってもよいことは、後述する通りである。そして、クライアント装置４０が送信した要求に対し、サーバ装置３０が必要な処理を行って応答を返すことにより、クライアント・サーバシステムとして機能する。証明書管理装置１０は、上記の認証処理に用いるデジタル証明書を発行し、またそのデジタル証明書の管理や更新等を行うための装置であり、ＣＡに相当する。

【００４６】

なお、実際のシステムにおいては、サーバ装置３０がクライアントの機能を併せ持ったり、クライアント装置４０がサーバの機能を併せ持ったりすることも考えられる。そして、サーバ装置３０がクライアントとして機能して、サーバとして機能するクライアント装置４０に要求を送信することもありうるが、このような場合には、後述する第２の実施形態に準ずる動作を行うようにすればよい。従って、ここでは後述するルート鍵更新処理においてサーバとして機能する装置をサーバ装置、クライアントとして機能する装置をクライアント装置と呼ぶものとする。

【００４７】

このようなデジタル証明書管理システムにおいて、上述のクライアント装置４０からサーバ装置３０への送信も含め、証明書管理装置１０，サーバ装置３０，クライアント装置４０の各ノードは、ＲＰＣ（remote procedure call）により、相互の実装するアプリケーションプログラムのメソッドに対する処理の依頼である「要求」を送信し、この依頼された処理の結果である「応答」を取得することができるようになっている。

【００４８】

すなわち、サーバ装置３０又はクライアント装置４０では、証明書管理装置１０への要求を生成してこれを証明書管理装置１０へ引き渡し、この要求に対する応答を取得できる一方で、証明書管理装置１０は、クライアント・サーバシステム側への要求を生成してこれをサーバ装置３０へ引き渡し、この要求に対する応答を取得できるようになっている。この要求には、サーバ装置３０にクライアント装置４０に対して各種要求を送信させ、クライアント装置４０からの応答をサーバ装置３０を介して取得することも含まれる。

なお、ＲＰＣを実現するために、ＳＯＡＰ（Simple Object Access Protocol），ＨＴＴＰ（Hyper Text Transfer Protocol），ＦＴＰ（File Transfer Protocol），ＣＯＭ（Component Object Model），ＣＯＲＢＡ（Common Object Request Broker Architecture）等の既知のプロトコル（通信規格），技術，仕様などを利用することができる。

【００４９】

この送受信のデータ送受モデルを図３の概念図に示す。

（Ａ）は、証明書管理装置１０でクライアント装置４０に対する要求が発生したケース

である。このケースでは、証明書管理装置１０が管理装置側要求ａを生成し、これをサーバ装置３０を経由して受け取ったクライアント装置４０がこの要求に対する応答ａを返すというモデルになる。なお、（Ａ）では、応答ａだけでなく応答遅延通知ａ′を返信するケースが表記されている。これは、クライアント装置４０が、サーバ装置３０を経由して管理装置側要求ａを受け取って、当該要求に対する応答を即座に返せないと判断したときには、応答遅延通知を通知して一旦接続状態を切断し、次回の接続の際に上記要求に対する応答を改めて引き渡す構成としているためである。

なおここでは、サーバ装置３０からクライアント装置４０に対して通信を要求することはできないので、サーバ装置３０からクライアント装置４０に対して送信すべき要求は、クライアント装置４０からサーバ装置３０に対して接続要求があった場合に、これに対する応答として送信することになる。

【００５０】

（Ｂ）は、クライアント装置４０で証明書管理装置１０に対する要求が発生したケースである。このケースでは、クライアント装置４０がクライアント装置側要求ｂを生成し、これをサーバ装置３０を経由して受け取った証明書管理装置１０が、当該要求に対する応答ｂを返すというモデルになっている。なお、（Ｂ）のケースでも、応答を即座に返せないときに応答遅延通知ｂ′を返すことは（Ａ）のケースと同様である。

【００５１】

次に、このデジタル証明書管理システムを構成する各装置の構成と機能についてより詳細に説明する。

図１は、図２に示した証明書管理装置のハードウェア構成を示すブロック図である。この図に示す通り、証明書管理装置１０は、ＣＰＵ１１，ＲＯＭ１２，ＲＡＭ１３，ＨＤＤ１４，通信インタフェース（Ｉ／Ｆ）１５を備え、これらがシステムバス１６によって接続されている。そして、ＣＰＵ１１がＲＯＭ１２やＨＤＤ１４に記憶している各種制御プログラムを実行することによってこの証明書管理装置１０の動作を制御し、後述するように各手段（証明鍵更新手段，第１の送信手段，第２の送信手段，その他の手段）として機能させる。

なお、証明書管理装置１０のハードウェアとしては、適宜公知のコンピュータを採用することができる。もちろん、必要に応じて他のハードウェアを付加してもよい。

【００５２】

クライアント・サーバシステムを構成するクライアント装置及びサーバ装置については、装置の遠隔管理，電子商取引等の目的に応じて種々の構成をとることができる。例えば、遠隔管理の場合には、プリンタ，ＦＡＸ装置，コピー機，スキャナ，デジタル複合機等の画像処理装置を始め、ネットワーク家電，自動販売機，医療機器，電源装置，空調システム，ガス・水道・電気等の計量システム等の電子装置を被管理装置であるサーバ装置とし、これらの被管理装置から情報を収集したり、コマンドを送って動作させたりするための管理装置をクライアント装置とすることが考えられる。

【００５３】

しかし、クライアント装置及びサーバ装置は、少なくともそれぞれＣＰＵ，ＲＯＭ，ＲＡＭ，ネットワークを介して外部装置と通信するための通信Ｉ／Ｆ、および認証処理に必要な情報を記憶する記憶手段を備え、ＣＰＵがＲＯＭ等に記憶した所要の制御プログラムを実行することにより、装置をクライアントあるいはサーバとして機能させることができるものとする。

なお、この通信には、有線，無線を問わず、ネットワークを構築可能な各種通信回線（通信経路）を採用することができる。証明書管理装置１０との間の通信についても同様である。

【００５４】

図２には、上述のように、各装置のこの実施形態の特徴となる部分の機能構成を示している。

まず、証明書管理装置１０は、証明用鍵作成部２１，証明書発行部２２，証明書管理部

２３，証明書更新部２４，通信機能部２５を備えている。

証明用鍵作成部２１は、デジタル署名の作成に用いる証明用私有鍵であるルート私有鍵と、そのデジタル証明書の正当性を確認するための、ルート私有鍵と対応する証明用公開鍵（証明鍵）であるルート鍵とを作成する証明用鍵作成手段の機能を有する。

【００５５】

証明書発行部２２は、サーバ装置３０とクライアント装置４０との間の認証処理に用いる認証情報であるクライアント公開鍵およびサーバ公開鍵にデジタル署名を付して、デジタル証明書であるクライアント公開鍵証明書およびサーバ公開鍵証明書として発行する証明書発行手段の機能を有する。また、クライアント公開鍵，クライアント私有鍵，サーバ公開鍵，サーバ私有鍵の作成及び、ルート鍵にデジタル署名を付したデジタル証明書であるルート鍵証明書の作成も、この証明書発行部２２の機能である。

証明書管理部２３は、証明書発行部２２が発行したデジタル証明書、その作成に用いたルート私有鍵、およびそのルート私有鍵と対応するルート鍵を管理する証明書管理手段の機能を有する。そして、これらの証明書や鍵を、その有効期限や発行先、ＩＤ、更新の有無等の情報と共に記憶する。

【００５６】

証明書更新部２４は、ルート鍵の更新を行う場合に、有効なルート私有鍵の各々について、新たなルート私有鍵（新ルート私有鍵）及びこれと対応する新たなルート鍵（新ルート鍵）を証明用鍵作成部２１に作成させ、これらを更新する証明用鍵更新手段の機能を有する。さらに、この更新に当たって、証明書発行部２２に新ルート私有鍵を用いてデジタル署名を付した新たなクライアント公開鍵証明書（新クライアント公開鍵証明書）、新たなサーバ公開鍵証明書（新サーバ公開鍵証明書）及び新たなルート鍵証明書（新ルート鍵証明書）を発行させ、通信機能部２５によってこれらをサーバ装置３０及びクライアント装置４０に送信させ、サーバ装置３０及びクライアント装置４０にこれらの更新を要求させる機能も有する。また、詳細は後述するが、更新に必要な各処理の手順や進捗状況の管理も証明書更新部２４が行う。

【００５７】

通信機能部２５は、ネットワークを介して外部装置と通信する機能を有し、証明書管理部２３の指示に応じて必要なデータをサーバ装置３０及びクライアント装置４０に送信したり、受信したデータを証明書更新部２４に渡したりする。

そして、これらの各部の機能は、図１に示したＣＰＵ１１が所要の制御プログラムを実行して証明書管理装置１０の各部の動作を制御することにより実現される。

【００５８】

一方、サーバ装置３０は、証明書記憶部３１，通信機能部３２，サーバ機能部３３を備えている。

証明書記憶部３１は、ＳＳＬによる認証処理に用いる鍵を記憶する機能を有し、例えば相互認証を行う場合には、ルート鍵証明書、サーバ私有鍵、およびサーバ公開鍵証明書を記憶する。

通信機能部３２は、ネットワークを介して外部装置と通信する機能を有し、受信したデータをサーバ機能部３３に渡し、またサーバ機能部３３の指示に従ってデータを外部装置に送信する。

【００５９】

サーバ機能部３３は、クライアント装置４０から受信した要求に対して所要の処理を行って応答を返すサーバとしての機能を有する。また、以下に詳述するが、証明書管理装置１０から受信した証明書更新等の要求に対しても、所要の処理を行って応答を返す。

そして、これらの各部の機能は、サーバ装置３０のＣＰＵが所要の制御プログラムを実行してサーバ装置３０の各部の動作を制御することにより実現される。

【００６０】

また、クライアント装置４０は、証明書記憶部４１，通信機能部４２，クライアント機能部４３を備えている。

証明書記憶部４１は、ＳＳＬによる認証処理に用いる鍵を記憶する機能を有し、例えば相互認証を行う場合には、ルート鍵証明書、クライアント私有鍵、およびクライアント公開鍵証明書を記憶する。

通信機能部４２は、ネットワークを介して外部装置と通信する機能を有し、受信したデータをクライアント機能部４３に渡し、またクライアント機能部４３の指示に従ってデータを外部装置に送信する。

【００６１】

クライアント機能部４３は、ユーザからの操作、図示しないセンサが検出した状態変化、あるいは図示しないタイマによって計測した所定時間経過等をトリガとして、サーバ装置３０に対して所要の要求を送信し、サーバ装置３０からこれに対する応答を受信した場合にはその内容に従った処理を行うクライアントとしての機能を有する。また、以下に詳述するが、応答として証明書管理装置１０からの証明書更新等の要求を受信した場合には、所要の処理を行って応答を返す。

そして、これらの各部の機能は、クライアント装置４０のＣＰＵが所要の制御プログラムを実行してクライアント装置４０の各部の動作を制御することにより実現される。

【００６２】

なお、このデジタル証明書管理装置において、証明書管理装置１０が直接通信可能なのは、クライアント・サーバシステムを構成する装置のうちサーバ装置３０のみであり、証明書管理装置１０からクライアント装置４０に対する要求は、サーバ装置３０が中継して送るものとする。クライアント装置４０から証明書管理装置１０への応答も、同様である。

また、上記のサーバ装置３０及びクライアント装置４０には、工場出荷時あるいはそれに順ずる時期、少なくともユーザが認証処理の運用を開始する前に、初めのルート鍵を記憶させておくものとする。このとき、公開鍵証明書及び私有鍵も共に記憶させるようにするとよい。

【００６３】

次に、このような基本的な機能を有する図２に示したデジタル証明書管理システムにおけるこの実施形態の特徴に関連する処理である、ルート鍵更新処理およびそのために必要な構成について説明する。

なお、以下の説明に用いるシーケンス図に記載するサーバ装置３０とクライアント装置４０と間の通信処理に際しては、個々に図示はしていないが、通信の確立前にＳＳＬによる認証処理を行い、認証が成功した場合のみ、そのＳＳＬによって確保した通信経路でデータの転送を行うものとする。そして、この認証処理に支障を来さないようにルート鍵証明書を更新可能であることが、この実施形態の特徴である。なお、更新に際しての認証は、認証を行おうとする時点で記憶しているルート鍵や公開鍵証明書を用いて行うことになる。すなわち、更新前は更新前のものを、更新後には更新後のものを用いて認証を行うことになる。

またここでは、証明書管理装置１０とサーバ装置３０との間の通信は、直通回線等の、安全（データの改竄や盗聴がなされないこと）を確保できる通信経路を介して行うものとする。

【００６４】

ここで、まず、上述のＳＳＬを用いて認証処理を行う場合の通信手順について説明する。この認証処理としては、互いが互いを認証する相互認証と、一方が他方を認証する片方向認証とが考えられ、各実施形態においてどちらの方式を採用してもよいが、まず、相互認証について説明する。

図４に、クライアント装置とサーバ装置とがＳＳＬによる相互認証を行う際の各装置において実行する処理のフローチャートを、その処理に用いる情報と共に示す図である。

図４に示すように、ＳＳＬによる相互認証を行う際には、まずクライアント装置４０側にルート鍵証明書，クライアント私有鍵，クライアント公開鍵証明書（クライアント証明書）を記憶させておく。クライアント私有鍵は、証明書管理装置１０がクライアント装置

４０に対して発行した私有鍵である。そして、クライアント公開鍵証明書は、その私有鍵と対応する公開鍵に証明書管理装置１０がデジタル署名を付してデジタル証明書としたものである。また、ルート鍵証明書は、証明書管理装置１０がデジタル署名に用いた証明用私有鍵であるルート私有鍵と対応する証明用公開鍵（以下「証明鍵」ともいう）であるルート鍵に、デジタル署名を付してデジタル証明書としたものである。

【００６５】

また、サーバ装置３０側には、ルート鍵証明書，サーバ私有鍵，サーバ公開鍵証明書（サーバ証明書）を記憶させておく。サーバ私有鍵及びサーバ公開鍵証明書は、証明書管理装置１０がサーバ装置３０に対して発行した私有鍵及び公開鍵証明書である。ここではクライアント装置４０とサーバ装置３０に対して同じ証明書管理装置１０が同じルート私有鍵を用いて証明書を発行しているものとし、従ってルート鍵証明書はクライアント装置４０とサーバ装置３０で共通となる。

これらの各鍵や証明書の関係は、背景技術の項で図４１を用いて説明した通りである。

【００６６】

フローチャートの説明に入る。なお、図４において、２本のフローチャート間の矢印は、データの転送を示し、送信側は矢印の根元のステップで転送処理を行い、受信側はその情報を受信すると矢印の先端のステップの処理を行うものとする。また、各ステップの処理が正常に完了しなかった場合には、その時点で認証失敗の応答を返して処理を中断するものとする。相手から認証失敗の応答を受けた場合、処理がタイムアウトした場合等も同様である。

【００６７】

クライアント装置４０のＣＰＵは、サーバ装置３０に通信を要求する場合、所要の制御プログラムを実行することにより、図４の左側に示すフローチャートの処理を開始する。そして、ステップＳ１１でサーバ装置に対して接続要求を送信する。

一方サーバ装置３０のＣＰＵは、この接続要求を受信すると、所要の制御プログラムを実行することにより、図４の右側に示すフローチャートの処理を開始する。そして、ステップＳ２１で第１の乱数を生成し、これをサーバ私有鍵を用いて暗号化する。そして、ステップＳ２２でその暗号化した第１の乱数とサーバ公開鍵証明書とをクライアント装置４０に送信する。

【００６８】

クライアント装置４０側では、これを受信すると、ステップＳ１２でルート鍵証明書を用いてサーバ公開鍵証明書の正当性を確認する。これには、損傷や改竄を受けていないことを確認するのみならず、書誌情報を参照してサーバ装置３０が適当な通信相手であることを確認する処理を含む。

そして確認ができると、ステップＳ１３で、受信したサーバ公開鍵証明書に含まれるサーバ公開鍵を用いて第１の乱数を復号化する。ここで復号化が成功すれば、第１の乱数は確かにサーバ公開鍵証明書の発行対象であるサーバ装置３０から受信したものだと確認できる。そして、サーバ装置３０を正当な通信相手として認証する。

【００６９】

その後、ステップＳ１４でこれとは別に第２の乱数及び第３の乱数を生成する。そして、ステップＳ１５で第２の乱数をクライアント私有鍵を用いて暗号化し、第３の乱数をサーバ公開鍵を用いて暗号化し、ステップＳ１６でこれらをクライアント公開鍵証明書と共にサーバ装置３０に送信する。第３の乱数の暗号化は、サーバ装置３０以外の装置に乱数を知られないようにするために行うものである。

【００７０】

サーバ装置３０側では、これを受信すると、ステップＳ２３でルート鍵証明書を用いてクライアント公開鍵証明書の正当性を確認する。これにも、ステップＳ１２の場合と同様、クライアント装置４０が適当な通信相手であることを確認する処理を含む。そして確認ができると、ステップＳ２４で、受信したクライアント公開鍵証明書に含まれるクライアント公開鍵を用いて第２の乱数を復号化する。ここで復号化が成功すれば、第２の乱数は

確かにクライアント公開鍵証明書の発行対象であるクライアント装置４０から受信したものだと確認できる。そして、クライアント装置４０を正当な通信相手として認証する。

【００７１】

その後、ステップＳ２５でサーバ私有鍵を用いて第３の乱数を復号化する。ここまでの処理で、サーバ側とクライアント側に共通の第１乃至第３の乱数が共有されたことになる。そして、少なくとも第３の乱数は、生成したクライアント装置４０と、サーバ私有鍵を持つサーバ装置３０以外の装置が知ることはない。ここまでの処理が成功すると、ステップＳ２６でクライアント装置４０に対して認証成功の応答を返す。

【００７２】

クライアント装置４０側では、これを受信すると、ステップＳ１７で第１乃至第３の乱数から共通鍵を生成し、以後の通信の暗号化に用いるものとして認証処理を終了する。サーバ装置３０側でも、ステップＳ２７で同様の処理を行って終了する。そして、以上の処理によって互いに通信を確立し、以後はステップＳ１７又はＳ２７で生成した共通鍵を用い、共通鍵暗号方式でデータを暗号化して通信を行う。

このような処理を行うことにより、クライアント装置４０とサーバ装置３０が互いに相手を認証した上で安全に共通鍵を交換することができ、通信を確かな相手と安全に行うことができる。

【００７３】

なお、片方向認証の場合、図４に示した処理は、図５に示すように簡略化することができる。すなわち、この場合には、第２の乱数をクライアント私有鍵で暗号化し、公開鍵証明書Ａを通信装置Ｂに送信することは必須ではない。この場合、サーバ装置３０側のステップＳ２３及びＳ２４の処理は不要になる。このようにすると、サーバ装置３０がクライアント装置４０を認証することはできないが、クライアント装置４０がサーバ装置３０を認証するだけでよい場合にはこの処理で十分である。

そしてこの場合には、クライアント装置４０に記憶させるのはルート鍵証明書のみでよく、クライアント私有鍵及びクライアント公開鍵証明書は不要である。また、サーバ装置３０にはルート鍵証明書を記憶させる必要はない。従ってこの場合、以下に説明する各ルート鍵証明書の更新処理も、クライアント装置４０のルート鍵証明書とサーバ装置３０のサーバ公開鍵証明書のみを更新する処理に簡略化することが可能である。

【００７４】

次に、ルート鍵証明書の更新処理の説明に移るが、ここで説明するルート鍵更新処理は、この発明のデジタル証明書管理方法の第１の実施形態に係る処理であり、図６乃至図１２のシーケンス図に示す処理を、図１３のフローチャートに示す順番で実行するものである。そこで、まず図６乃至図１２の各シーケンス図に示す処理の内容を説明してから、図１３を用いてその実行順について説明する。以下の各図に示す処理は、証明書管理装置１０，サーバ装置３０，クライアント装置４０の各ＣＰＵが、所要の制御プログラムを実行することによって行うものである。

【００７５】

まず図６のシーケンス図に処理Ｓとしてルート鍵証明書作成処理を示す。

この処理においては、証明書管理装置１０は、ステップＳ１０１で、有効なルート私有鍵について、新たなルート私有鍵とルート鍵のペアを作成する。ここで、「有効な」ルート私有鍵とは、その時点でクライアント・サーバシステムにおける認証処理に使用中のルート私有鍵という意味であり、より正確には、そのルート私有鍵を用いてデジタル署名を付した証明書が、認証処理に用いられる状態でサーバ装置３０又はクライアント装置４０に記憶されているものをいうものとする。過去に作成した私有鍵が有効か否かは、証明書管理部２３に記憶している公開鍵証明書及びルート鍵証明書の有効期限やその更新の有無の情報や、証明書に含まれる、デジタル署名に使用したルート私有鍵の識別情報等の情報を基に判断することができる。また、新たな鍵と置き換えられるべきそれまでの鍵を、「従前の」鍵と呼ぶことにする。証明書についても同様である。

そして、ステップＳ１０２で、ステップＳ１０１で作成した新ルート鍵に従前のルート

私有鍵を用いたデジタル署名を付し、第１の証明鍵証明書である配布用ルート鍵証明書を作成する。

以上がルート鍵証明書作成処理である。

【００７６】

次に、図７のシーケンス図に処理１としてサーバ装置のルート鍵証明書記憶処理を示す。

この処理においては、まずステップＳ１１１で、証明書管理装置１０がサーバ装置３０に対して、図６のステップＳ１０２で作成した配布用ルート鍵証明書と共に、その更新要求を送信する。この処理において、証明書管理装置１０のＣＰＵ１１が第２の送信手段として機能する。

【００７７】

サーバ装置３０は、この要求を受け取ると、ステップＳ１１２で従前のルート鍵証明書を用いて配布用ルート鍵証明書の正当性を確認する。上述のように、配布用ルート鍵証明書には、従前のルート私有鍵を用いたデジタル署名を付しているので、従前のルート鍵を用いてその内容を復号化し、確かに証明書管理装置１０によって発行されたものであることを確認できる。また、このとき、背景技術の項で図４１を用いて説明したようにルート鍵が損傷や改竄等を受けていないことも確認できる。従って、このような配布用ルート鍵証明書を用いることにより、受け取ったルート鍵の正当性を人手によらず確認できることになる。

そして、これが確認できると、次のステップＳ１１３で配布用ルート鍵証明書を証明書記憶部３１に記憶する。このとき、まだ従前のルート鍵証明書は消去しない。従って、証明書記憶部３１には２つのルート鍵証明書が記憶された状態となる。

【００７８】

この状態で認証処理を行う場合、受信した公開鍵証明書の正当性を確認する際には、２つのルート鍵証明書を順次用いて確認を試み、どちらかのルート鍵証明書を用いて確認が成功すれば、正当性が確認できたものとする。従って、新旧どちらのルート私有鍵を用いてデジタル署名を付したデジタル証明書であっても、その正当性を確認することができる。なお、配布用ルート鍵証明書を認証処理に使用する際の、ルート鍵に破損や改竄がないことの確認は、従前のルート鍵証明書を用いて行うことができる。これらのステップＳ１１２及びＳ１１３において、サーバ装置３０のＣＰＵが第２のサーバ側更新手段として機能する。

サーバ装置３０はその後、ステップＳ１１４で証明書管理装置１０に対して更新要求に対する応答として結果通知を返し、配布用ルート鍵証明書の記憶が成功していればその旨を、何らかの理由で失敗していればその旨を伝える。なお、この結果通知は、少なくともサーバ装置３０が配布用ルート鍵証明書を受信したことを示す情報である。以下の結果通知も同様な意味を持つものとする。

以上がサーバ装置のルート鍵証明書記憶処理である。

【００７９】

次に、図８のシーケンス図に処理２としてクライアント装置のルート鍵証明書記憶処理を示す。

この処理においては、まずステップＳ１２１で、証明書管理装置１０がサーバ装置３０に対して、図６のステップＳ１０２で作成した配布用ルート鍵証明書と共に、その更新要求をクライアント装置４０に送信するよう要求する更新要求送信要求を送信する。サーバ装置３０は、これに応じてクライアント装置４０に対して配布用ルート鍵証明書とその更新要求とを送信するのであるが、サーバ装置３０側から送信要求を行うことはできない。そこで、クライアント装置４０が所定のタイミングで定期的にサーバ装置３０に対して通信要求を送信するようにし（Ｓ１２２）、これに対する応答として配布用ルート鍵証明書とその更新要求とを送信するようにしている（Ｓ１２３）。

【００８０】

なお、クライアント装置４０がサーバ装置３０に対する通信要求をＨＴＴＰリクエスト

として送信し、サーバ装置３０からクライアント装置４０に対して送信する要求やデータをこれに対する応答であるＨＴＴＰレスポンスとして送信するようにするとよい。このようにすれば、クライアント装置４０がファイアウォールの内側に設置されている場合でも、これを越えてサーバ装置３０からクライアント装置４０にデータを転送することができる。

【００８１】

ファイアウォールを越える手段はこれに限られるものではなく、例えば、ＳＭＴＰ（Simple Mail Transfer Protocol）を利用して、送信したいデータを記載あるいは添付したメールを送信することも考えられる。ただし、信頼性の面ではＨＴＴＰが優れている。

以上の処理により、証明書管理装置１０からクライアント装置４０に、サーバ装置３０を介して配布用ルート鍵証明書とその更新要求とが送信されることになり、ステップＳ１２１の処理においては、証明書管理装置１０のＣＰＵ１１が第１の送信手段として機能する。

【００８２】

クライアント装置４０は、この要求を受け取ると、ステップＳ１２４で従前のルート鍵証明書を用いて配布用ルート鍵証明書の正当性を確認する。そして、これが確認できると、次のステップＳ１２５で配布用ルート鍵証明書を証明書記憶部４１に記憶する。このとき、まだ従前のルート鍵証明書は消去しない。これらの確認と記憶の詳細については、図７のステップＳ１１２及びＳ１１３の場合と同様であり、これらのステップにおいて、クライアント装置４０のＣＰＵが第２のクライアント側更新手段として機能する。

クライアント装置４０はその後、ステップＳ１２６で証明書管理装置１０に対して更新要求に対する応答として結果通知を返すが、これはまずサーバ装置３０に対して送信し、サーバ装置３０がステップＳ１２７で証明書管理装置に対して送信する。

以上がクライアント装置のルート鍵証明書記憶処理である。

【００８３】

次に、図９のシーケンス図に処理３としてクライアント装置の公開鍵証明書記憶処理を示す。

この処理においてはまずステップＳ１３１で、証明書管理装置１０が、クライアント装置４０に対して発行してあるクライアント公開鍵に、新ルート私有鍵を用いたデジタル署名を付して新クライアント公開鍵証明書を作成する。なお、クライアント私有鍵は更新しないので、クライアント公開鍵自体も更新する必要はない。

【００８４】

そしてステップＳ１３２で、証明書管理装置１０がサーバ装置３０に対して、ステップＳ１３１で作成した新クライアント公開鍵証明書と共に、その更新要求をクライアント装置４０に送信するよう要求する更新要求送信要求を送信する。サーバ装置３０は、これに応じて、図８のステップＳ１２２及びＳ１２３の場合と同様に、クライアント装置４０からの通信要求（Ｓ１３３）に対する応答として新クライアント公開鍵証明書とその更新要求とを送信するようにしている（Ｓ１３４）。

以上の処理により、証明書管理装置１０からクライアント装置４０にサーバ装置３０を介して新クライアント公開鍵証明書とその更新要求とが送信されることになり、ステップＳ１３２の処理においては、証明書管理装置１０のＣＰＵ１１が第１の送信手段として機能する。

【００８５】

クライアント装置４０は、この要求を受け取るとステップＳ１３５で、図８のステップＳ１２５で記憶した配布用ルート鍵証明書を用いて新クライアント公開鍵証明書の正当性を確認する。上述のように、新クライアント公開鍵証明書には、新ルート私有鍵を用いたデジタル署名を付しているので、配布用ルート鍵証明書に含まれる新ルート鍵を用いてその内容を復号化し、確かに証明書管理装置１０によってクライアント装置４０に対して発行されたものであることを確認できる。そして、これが確認できると、次のステップＳ１３６で新クライアント公開鍵証明書を証明書記憶部４１に記憶する。これらのステップＳ

１３５及びＳ１３６において、クライアント装置４０のＣＰＵが第１のクライアント側更新手段として機能する。

【００８６】

このとき、まだ従前のクライアント公開鍵証明書は消去しない。従って、証明書記憶部４１には２つのクライアント公開鍵証明書が記憶された状態となる。この状態で認証処理を行い、通信相手に対して公開鍵証明書を送信する場合には、まず新公開鍵証明書を送信するものとする。

この場合、通信相手が既に新ルート鍵を（配布用ルート鍵証明書又は後述する新ルート鍵証明書として）記憶していれば、新公開鍵証明書のデジタル署名を復号化できるので、問題なく認証を受けることができる。一方、通信相手がまた新ルート鍵を記憶していない場合には、新公開鍵証明書のデジタル署名を復号化できず、認証が失敗した旨の応答を受けることになる。しかしこの場合でも、再度通信を要求し、この際に従前の公開鍵証明書を送信するようにすれば、従前のルート鍵によってそこに付されたデジタル署名を復号化できるので、問題なく認証を受けることができる。

【００８７】

従って、２つの公開鍵証明書を記憶しておけば、通信相手が新ルート鍵を記憶していない場合に多少のオーバーヘッドが生じることはあるが、問題なく認証処理を行うことができる。なお、２つの公開鍵証明書に含まれる公開鍵本体は同じものであるので、クライアント私有鍵を用いて暗号化したデータの復号化は、どちらの公開鍵証明書を用いた場合でも同じように行うことができる。

クライアント装置４０はその後、ステップＳ１３７で証明書管理装置１０に対して更新要求に対する応答として結果通知を返すが、これはまずサーバ装置３０に対して送信し、サーバ装置３０がステップＳ１３８で証明書管理装置に対して送信する。

以上がクライアント装置の公開鍵証明書記憶処理である。

【００８８】

次に、図１０のシーケンス図に処理４としてサーバ装置の公開鍵証明書記憶処理を示す。

この処理においてはまずステップＳ１４１で、証明書管理装置１０が、クライアント装置４０に対して発行してあるサーバ公開鍵に、新ルート私有鍵を用いたデジタル署名を付して新サーバ公開鍵証明書を作成する。サーバ公開鍵自体の更新が不要であることは、上述のクライアント公開鍵の場合と同様である。

そしてステップＳ１４２で、証明書管理装置１０がサーバ装置３０に対して、新サーバ公開鍵証明書と共にその更新要求を送信する。この処理において、証明書管理装置１０のＣＰＵ１１が第２の送信手段として機能する。

【００８９】

サーバ装置３０は、この要求を受け取るとステップＳ１４３で、図７のステップＳ１１３で記憶した配布用ルート鍵証明書を用いて新公開鍵証明書の正当性を確認する。この点については、図９のステップＳ１３５の場合と同様である。そして、これが確認できると、次のステップＳ１４４で新サーバ公開鍵証明書を証明書記憶部４１に記憶し、従前のサーバ公開鍵証明書と置き換える。これらのステップＳ１４３及びＳ１４４において、サーバ装置３０のＣＰＵが第１のサーバ側更新手段として機能する。

【００９０】

ところで、サーバ装置３０の場合には、クライアント装置４０の場合と異なり、新公開鍵証明書を記憶させる場合に従前のものに追加するのではなくこれと置き換える必要があるのであるが、ここでこの点について説明する。

サーバ装置３０の場合には、クライアント装置４０から接続要求があった場合に公開鍵証明書をクライアント装置４０に送信するのであるが、サーバ公開鍵証明書を複数記憶していたとすると、送信毎にそのうちいずれかを選択して送信することになる。そして、クライアント装置４０側でデジタル証明書を復号化できないようなサーバ公開鍵証明書を送信してしまった場合には、認証は失敗することになる。例えば、クライアント装置４０が

新ルート鍵を記憶する前に新サーバ公開鍵証明書を送信した場合等である。

【００９１】

たとえ失敗したとしても、次に接続要求があった場合にもう一方のサーバ公開鍵証明書を送信すればよいという考え方もあるが、不特定多数のクライアント装置から任意のタイミングで接続要求を受け得るサーバ装置の場合、クライアント装置毎に送信すべきサーバ公開鍵証明書を選択することは、現実的ではない。また、クライアント装置がどのような装置であるかは、サーバ装置側では認証が済むまで通常わからないので、最初に送信するサーバ公開鍵証明書を適切に選択することも困難である。従って、サーバ装置にはサーバ公開鍵証明書を１つだけ記憶させ、クライアント装置から接続要求を受けた場合には常にこれを送信するようにする必要があるのである。

【００９２】

従って、サーバ装置３０では新サーバ公開鍵証明書を記憶させた時点で従前のサーバ公開鍵証明書は削除してしまうので、クライアント装置４０に新ルート鍵を記憶させる前にこれを行ってしまうと、クライアント装置側でサーバ公開鍵証明書のデジタル署名を復号化できなくなり、認証処理を行えなくなってしまう。そこで、サーバ装置３０の公開鍵証明書記憶処理は、クライアント装置のルート鍵証明書記憶処理の完了後に行う必要がある。

以上のようなステップＳ１４４の終了後、サーバ装置３０はステップＳ１４５で証明書管理装置１０に対して更新要求に対する応答として結果通知を返し、新サーバ公開鍵証明書の記憶が成功していればその旨を、何らかの理由で失敗していればその旨を伝える。

以上がサーバ装置の公開鍵証明書記憶処理である。

【００９３】

次に、図１１のシーケンス図に処理５としてサーバ装置のルート鍵証明書書き換え処理を示す。

この処理においてはまずステップＳ１５１で、証明書管理装置１０が、新ルート鍵に新ルート私有鍵を用いたデジタル署名を付して第２の証明鍵証明書として新ルート鍵証明書を作成する。そして、ステップＳ１５２で証明書管理装置１０がサーバ装置３０に対して、新ルート鍵証明書と共にその更新要求を送信する。この処理においても、証明書管理装置１０のＣＰＵ１１が第２の送信手段として機能する。

【００９４】

サーバ装置３０は、この要求を受け取ると、ステップＳ１５３で配布用ルート鍵証明書を用いて新ルート鍵証明書の正当性を確認する。上述のように、新ルート鍵証明書には、新ルート私有鍵を用いたデジタル署名を付しているので、配布用ルート鍵証明書に含まれる新ルート鍵を用いてその内容を復号化し、確かに証明書管理装置１０によって発行されたものであることを確認できる。

そして、これが確認できると、次のステップＳ１５４で新ルート鍵証明書を証明書記憶部３１に記憶する。そして、配布用ルート鍵証明書及び従前のルート鍵証明書を削除して廃棄し、ルート鍵証明書を新たなものに書き換えてしまう。このようにすると、従前のルート私有鍵を用いてデジタル署名を付したデジタル証明書は復号化できなくなってしまうが、クライアント装置４０に新クライアント公開鍵証明書を記憶させた後であれば、クライアント装置４０から送られてくる公開鍵証明書の確認には支障がないので、認証処理に支障を来すことはない。

【００９５】

サーバ装置３０はその後、ステップＳ１５５で証明書管理装置１０に対して更新要求に対する応答として結果通知を返し、新ルート鍵証明書の記憶が成功していればその旨を、何らかの理由で失敗していればその旨を伝える。

以上がサーバ装置のルート鍵証明書書き換え処理である。

【００９６】

次に、図１２のシーケンス図に処理６としてクライアント装置のルート鍵証明書書き換え処理を示す。

この処理においてはまずステップＳ１６１で、証明書管理装置１０が、新ルート鍵に新ルート私有鍵を用いたデジタル署名を付して第２の証明鍵証明書として新ルート鍵証明書を作成する。これは、図１１のステップＳ１５１で作成するものと同じであるので、ここで作成したものを流用してもよい。逆に図１１のステップＳ１５１で、このステップＳ１６１で作成したものを流用してもよい。

【００９７】

そしてステップＳ１６２で、証明書管理装置１０がサーバ装置３０に対して、ステップＳ１６１で作成した新ルート鍵証明書と共に、その更新要求をクライアント装置４０に送信するよう要求する更新要求送信要求を送信する。サーバ装置３０は、これに応じて、図８のステップＳ１２２及びＳ１２３の場合と同様に、クライアント装置４０からの通信要求（Ｓ１６３）に対する応答として新ルート鍵証明書とその更新要求とを送信するようにしている（Ｓ１６４）。

以上の処理により、証明書管理装置１０からクライアント装置４０にサーバ装置３０を介して新ルート鍵証明書とその更新要求とが送信されることになり、ステップＳ１６２の処理においても、証明書管理装置１０のＣＰＵ１１が第１の送信手段として機能する。

【００９８】

クライアント装置４０は、この要求を受け取ると、ステップＳ１６５で配布用ルート鍵証明書を用いて新ルート鍵証明書の正当性を確認する。そして、これが確認できると、次のステップＳ１６６で新ルート鍵証明書を証明書記憶部４１に記憶する。そして、配布用ルート鍵証明書及び従前のルート鍵証明書を削除して廃棄し、ルート鍵証明書を新たなものに書き換えてしまう。これらの処理については、図１１のステップＳ１５３及びＳ１５４の場合と同様である。ただし、クライアント装置４０への新クライアント公開鍵証明書の記憶が済んでいれば、ステップＳ１６６で従前のクライアント公開鍵証明書も同時に廃棄してしまってよい。

【００９９】

クライアント装置４０はその後、ステップＳ１６７で証明書管理装置１０に対して更新要求に対する応答として結果通知を返すが、これはまずサーバ装置３０に対して送信し、サーバ装置３０がステップＳ１６８で証明書管理装置に対して送信する。

以上がクライアント装置のルート鍵証明書書き換え処理である。

【０１００】

以上の図６乃至図１２に示した各処理の実行タイミングは、証明書管理装置１０の証明書更新部２４が、図１３に示すフローチャートに従って管理する。すなわち、ルート鍵の更新事由を検出した場合に、図１３のフローチャートに示す処理を開始し、まず図６に示した処理Ｓを実行し、その後処理１乃至処理６を実行する。なお、ルート鍵の更新事由としては、所定の有効期限の到来、管理者の指示等が考えられる。管理者が更新の指示を行う場合としては、ルート私有鍵の第３者への漏洩が判明した場合等が考えられる。

また、図１３において、矢印の先の処理は、矢印の根元側の処理が全て完了してから開始する。破線で示した矢印については、その条件は必須ではないが考慮した方が好ましいということを示す。

【０１０１】

具体的には、処理１及び処理２は処理Ｓの完了後に開始する。処理３は、処理２の完了後に開始するが、処理１も完了した後に開始する方が好ましい。処理４は、処理１及び処理２の完了後に開始する。処理５は、処理１及び処理３の完了後に開始する。処理６は、処理２及び処理４の完了後に開始する。そして、処理３乃至６が全て完了した時点で、ルート鍵及び公開鍵証明書の更新が終了したことになる。

なお、各処理は、更新要求に対する更新成功の応答を受け取った場合に完了したものとすることができる。この応答が、更新すべき証明書を受信した旨を示す情報も含むことは、上述した通りである。更新失敗の応答を受け取った場合や処理がタイムアウトした場合には、再度同じ処理を試みるとよいが、所定回数続けて失敗した場合には更新処理全体が失敗したものとするとよい。

【０１０２】
また、ここでは、図７等に示したように、証明書管理装置１０がサーバ装置３０に更新要求を送信した場合、サーバ装置３０が受信した証明書等の記憶を完了してから結果通知を返す例について説明した。しかし、図１４に示すように、サーバ装置３０が更新要求を受信した場合に直ちに受信応答を返す（Ｓ１１１′）ようにしてもよい。このようにした場合、ステップＳ１１１′の受信応答が、証明書管理装置１０が送信した更新要求及び配布用ルート鍵証明書を正常に受信した旨の情報となる。また、ステップＳ１１４の結果通知は、更新の成否やその原因等を伝える情報となる。そして、この結果通知に対しても、証明書管理装置１０が受信応答を返す（Ｓ１１４′）ようにするとよい。このようにすれば、サーバ装置３０側でも、結果通知が正常に証明書管理装置１０に受信されたことが把握できる。

【０１０３】
また、サーバ装置３０とクライアント装置４０との間の通信についても、同様な手順とし、何らかの要求を受信した場合に、その送信元に対して直ちに受信応答を返し、結果通知についても、これを受信した場合にその送信元に対して直ちに受信応答を返すようにするとよい。図８に示したシーケンスに上記のような考え方を採り入れたシーケンスを図１５に示す。

なお、ステップＳ１２３′での受信応答が、クライアント装置４０が配布用ルート鍵証明書及び更新要求を受信した旨の情報となるが、図８に示したシーケンスに単に上記の考え方を採り入れたシーケンスでは、この情報はサーバ装置３０がステップＳ１２７の結果通知を行うまで証明書管理装置１０には伝わらない。

そこで、図１５に破線で示したように、サーバ装置３０が、クライアント装置４０からの受信応答があった後、送信の成否のみを送信結果通知として証明書管理装置１０へ通知するようにしてもよい。このようにすれば、クライアント装置４０への送信の成否を速やかに証明書管理装置１０に伝えることができる。

【０１０４】
また、以上のように結果通知を行うようにした場合、図１３を用いて説明したような各処理の実行タイミング管理において、証明書等の送信先から受信応答があった場合に、送信先において証明書の記憶や設定は滞りなく進行するであろうという予測の下に処理を先の段階に進めてしまうことも可能である。具体的には、処理１が全て完了しなくても、図１４のステップＳ１１１′に示したような受信応答があった場合に処理１が完了したものとみなして処理４の開始時期を決定するようにしてもよい。また、処理２が全て完了しなくても、図１５のステップＳＡに示したような送信結果通知があった場合に処理２が完了したものとみなして処理４の開始時期を決定するようにしてもよい。

また、ここでは、図１４及び図１５に、それぞれ図７及び図８のシーケンスの変形例を示したのみであるが、以上のような考え方は、以降の実施例及び変形例に示すものも含め、全ての処理及びシーケンスに適用可能なものである。

【０１０５】
以上のようなタイミング管理に基づき、ルート鍵更新処理を図１３に示す手順で行う場合、サーバ装置３０とクライアント装置４０とは処理のどの時点であってもＳＳＬによる認証処理を行うことができるので、このように更新処理が途中で中断してしまっても、サーバ装置３０とクライアント装置４０との間の通信に大きな支障はない。従って、更新処理が失敗した場合に時間をかけて失敗の原因を特定した上で改めて更新処理を行っても、特に大きな問題はない。以後の各実施形態についても同様である。

【０１０６】
このデジタル証明書管理システムにおいては、ルート鍵更新処理をこのような手順で行うことにより、サーバ装置３０とクライアント装置４０との間の認証処理に大きな影響を与えることなく、ルート鍵を自動制御で更新することができる。また、従前の（更新前の）ルート鍵や公開鍵証明書を用いた認証を行ってＳＳＬによる通信経路を確保し、その通信経路で更新用の新ルート鍵や新公開鍵証明書を送信することができる。また、更新終了

後は、その新ルート鍵や新公開鍵証明書を用いた認証を行ってＳＳＬによる通信経路を確保できる状態にすることができる。従って、このようなデジタル証明書管理システムを用いることにより、ルート鍵更新用の特別な通信経路を用意せずにルート鍵を更新することができるので、通信に際してＳＳＬによる認証処理を行うクライアント・サーバシステムを、低コストで運用することができる。この点も、以後の各実施形態についても同様である。

【０１０７】

また、証明書管理装置１０とサーバ装置３０との間には、これとは別の安全な通信経路を設ける必要があるが、これは期限切れ等に伴う公開鍵証明書の更新のような、通常必要な処理に使用するものと共通の通信経路でよい。また、このような通信経路は証明書管理装置１０と１つの装置のみとの間に設ければよいので、特に大きな負担にはならない。証明書管理装置１０とサーバ装置３０とが物理的に近接している場合には専用ケーブルで結ぶ等してこのような経路を設けることは容易であり、この実施形態はこのような場合に好ましいものであると言える。

【０１０８】

図１３に示す処理手順において、この実施形態の特徴となるのは、まず、処理４（サーバ装置の公開鍵証明書記憶処理）を処理２（クライアント装置のルート鍵証明書記憶処理）の後で、すなわちクライアント装置４０から配布用ルート鍵証明書を受信した旨の応答があった後で実行する点である。

処理４の説明において上述したように、サーバ装置３０については公開鍵証明書を同時に２つ記憶させると不都合が生じるので、新サーバ公開鍵証明書を記憶させる際には従前のものを廃棄する必要があるのであるが、このような書き換えを行ってしまっても、クライアント装置４０に新ルート鍵を記憶させた後であれば、認証処理に支障が生じることがない。

【０１０９】

また、処理３（クライアント装置の公開鍵証明書記憶処理）を処理１（サーバ装置のルート鍵証明書記憶処理）の後で、すなわちサーバ装置３０から配布用ルート鍵証明書を記憶した旨の応答があった後で実行するようにするとよい。

処理３の説明で上述したように、クライアント装置４０に新クライアント公開鍵証明書を記憶させた時点でサーバ装置３０に新ルート鍵が記憶されていないと、サーバ装置３０に新ルート鍵が記憶されるまで通信にオーバーヘッドが生じ、効率が悪くなってしまうためである。

【０１１０】

処理５と処理６については、これらは必須の処理ではないが、従前のルート鍵証明書や公開鍵証明書をいつまでも記憶させておくとすると、記憶容量を無駄に消費することになる。鍵や証明書の記憶には、信頼性の高い記憶手段を用いることが好ましく、従って容量当たりのコストが高いので、この点は大きな問題になる。また、配布用ルート鍵証明書は、自己署名形式でないので、使用する際に従前のルート鍵証明書を参照する必要があり、処理効率が悪い。そこで、処理５と処理６を行って、ルート鍵証明書を自己署名形式のものにすると共に、従前の証明書を廃棄するようにするとよい。

【０１１１】

ルート鍵証明書を自己署名形式のものに書き換えるだけであれば、配布用ルート鍵証明書を記憶させた直後に、例えば処理５の場合には処理１の完了直後に行ってもよいのであるが、この時点では必ずしも従前のルート鍵証明書を廃棄できない。そして、この削除タイミングはサーバ装置３０側では決定することができないので、処理３の終了後に再度従前のルート鍵証明書を廃棄する要求を行う必要が生じてしまう。従って、処理１と処理３の完了後に処理５を行うことが、処理の簡略化の点から好ましい。処理６についても、同様の理由から処理２と処理４の完了後に行うことが好ましい。

【０１１２】

なお、ルート鍵は一旦記憶してしまえば一般に外部に送信する必要はないので、その後

の破損や改竄は考えにくいことから、ルート鍵証明書ではなく、鍵部分のみを記憶することも考えられる。このような場合には、配布用ルート鍵証明書に含まれる新ルート鍵を記憶してしまえばよいので、証明書管理装置１０から新ルート鍵証明書を別途送信する必要はない。そこで、このような場合、処理５，処理６においては、新ルート鍵証明書を送信せず、従前のルート鍵の廃棄のみを要求するようにすればよい。また、ルート鍵を使用する際に、デジタル署名の確認を行わないようにする場合についても同様である。

【０１１３】

また、この実施形態において、サーバ装置３０からクライアント装置４０への送信は、クライアント装置４０からの通信要求に対する応答として行う例について説明したが、サーバ装置３０がクライアントとしても機能できるようにし、クライアント装置４０がサーバとしても機能できるようにし、これらの機能によって、サーバ装置３０からクライアント装置４０へデータや要求を直接送信できるようにしてもよい。このような場合は、クライアント装置４０による通信要求は不要である。この点は、以下の実施形態においても同様である。

【０１１４】

〔第２の実施形態：図１６乃至図２３〕

次に、この発明によるデジタル証明書管理装置である証明書管理装置と、クライアント・サーバシステムを構成するクライアント装置及びサーバ装置とによって構成される、この発明のデジタル証明書管理システムの第２の実施形態の構成について説明する。

このデジタル証明書管理システムを構成する各装置の、この実施形態の特徴となる部分の機能構成を、図２と対応する図１６の機能ブロック図に示す。この図において、図２と対応する部分には同一の符号を付している。

【０１１５】

この図からわかるように、このデジタル証明書管理システムにおいてはまず、証明書管理装置１０をクライアント・サーバシステムを構成する装置のうちクライアント装置４０のみと直接通信可能とし、証明書管理装置１０からサーバ装置３０に対する要求は、クライアント装置４０が中継して送るものとした点が第１の実施形態と異なる。

また、クライアント装置４０にもサーバ機能部４４を設けた点も、第１の実施形態の場合と異なるが、このサーバ機能部４４は、受信した要求に対して所要の処理を行って応答を返すサーバとしての機能を有し、証明書管理装置１０との通信のために設けたものである。クライアント装置４０がクライアント機能部４３しか有しないとすると、証明書管理装置１０からクライアント装置４０にデータや要求等を送信する場合に、クライアント装置４０からの通信要求を待つ必要が生じてしまう。

【０１１６】

しかし、ルート鍵の更新処理は頻繁に行われるものではなく、例えば年に１回程度であるので、このためにクライアント装置４０が証明書管理装置１０に対して定期的に通信要求を行うとすると、ほとんどの通信が無駄になることになる。そこで、クライアント装置４０にサーバ機能部４４を設け、証明書管理装置１０側から通信を要求できるようにしたものである。このサーバ機能部４４の機能も、クライアント装置４０のＣＰＵが所要の制御プログラムを実行してクライアント装置４０の各部の動作を制御することにより実現されるものである。

【０１１７】

ただし、クライアント・サーバシステムを構成するサーバ装置３０との関係においては、クライアント装置４０は常にクライアントとして機能する。従って、証明書管理装置１０からサーバ装置３０への通信を仲介する場合には、通信機能部４２が証明書管理装置１０から受信したデータや要求を、サーバ機能部４４が受け取り、これをクライアント機能部４３に渡して、クライアント機能部４３の指示に基づいてサーバ装置３０に対する通信を要求してサーバ装置３０に送信することになる。サーバ装置３０からの応答を証明書管理装置１０に返す場合には、この逆の処理となる。

【０１１８】

これらの変更に伴ってルート鍵更新処理のシーケンスは変更されるが、それ以外の点については第１の実施形態と同様であるので、説明を省略する。

なおここでも、証明書管理装置１０とクライアント装置４０との間の通信は、直通回線等の、安全を確保できる通信経路を介して行うものとする。ただし、この実施形態の場合には、証明書管理装置１０とクライアント装置４０との間の通信にＳＳＬを用いることも可能であるが、この場合の構成については変形例として後述する。

【０１１９】

このデジタル証明書管理システムにおけるルート鍵更新動作は、この発明のデジタル証明書管理方法の第２の実施形態に係る動作であり、図１７乃至図２２のシーケンス図に示す処理及び図６を用いて上述した処理Ｓを、図２３のフローチャートに示す順番で実行するものである。そこで、まず図１７乃至図２２の各シーケンス図に示す処理の内容を説明してから、図２２を用いてその実行順について説明する。以下の各図に示す処理は、証明書管理装置１０，サーバ装置３０，クライアント装置４０の各ＣＰＵが、所要の制御プログラムを実行することによって行うものである。

【０１２０】

まず、図１７のシーケンス図に処理１１としてサーバ装置のルート鍵証明書記憶処理を示す。

この処理は、図７に示した処理１と同じ目的の処理であるが、ここでは証明書管理装置１０と直接通信する装置がクライアント装置４０であるため、手順が若干異なるものとなっている。

【０１２１】

すなわち、まずステップＳ２１１で、証明書管理装置１０がクライアント装置４０に対して、図６のステップＳ１０２で作成した配布用ルート鍵証明書と共に、その更新要求をサーバ装置３０に送信するよう要求する更新要求送信要求を送信する。そしてクライアント装置４０は、これに応じてサーバ装置３０に対して配布用ルート鍵証明書とその更新要求とを送信する（Ｓ２１２）。クライアント装置４０はサーバ装置３０に対して通信を要求できるので、図７の場合のように通信要求を待つ必要はない。

以上の処理により、証明書管理装置１０からサーバ装置３０にクライアント装置４０を介して配布用ルート鍵証明書とその更新要求とが送信されることになり、ステップＳ２１１の処理においては、証明書管理装置１０のＣＰＵ１１が第２の送信手段として機能する。

【０１２２】

サーバ装置３０は、ステップＳ２１２で送信されてきた更新要求を受け取ると、ステップＳ２１３で従前のルート鍵証明書を用いて配布用ルート鍵証明書の正当性を確認し、これが確認できると、次のステップＳ２１４で配布用ルート鍵証明書を証明書記憶部３１に記憶する。これらの処理は、図７のステップＳ１１２及びＳ１１３の処理と全く同じである。

【０１２３】

サーバ装置３０はその後、ステップＳ２１５で証明書管理装置１０に対して更新要求に対する応答として結果通知を返すが、これはまずクライアント装置４０に対して送信し、クライアント装置４０がステップＳ２１６で証明書管理装置に対して送信する。なお、この結果通知は、クライアント装置４０から受信した更新要求に対する応答として送信することができるので、クライアント装置４０からの通信要求を待つ必要はない。

以上がこの実施形態におけるサーバ装置のルート鍵証明書記憶処理である。

【０１２４】

次に、図１８のシーケンス図に処理１２としてクライアント装置のルート鍵証明書記憶処理を示す。

この処理は、図８に示した処理２と同じ目的の処理であるが、処理１１の場合と同様に手順が若干異なるものとなっている。

この処理においては、まずステップＳ２２１で、証明書管理装置１０がクライアント装

置４０に対して、図６のステップＳ１０２で作成した配布用ルート鍵証明書とその更新要求を送信する。この処理において、証明書管理装置１０のＣＰＵ１１が第１の送信手段として機能する。

【０１２５】

クライアント装置４０は、この要求を受け取ると、ステップＳ１２４で従前のルート鍵証明書を用いて配布用ルート鍵証明書の正当性を確認し、これが確認できると、次のステップＳ１２５で配布用ルート鍵証明書を証明書記憶部４１に記憶する。これらの処理は、図８のステップＳ１２４及びＳ１２５の処理と全く同じである。

クライアント装置４０はその後、ステップＳ２２４で証明書管理装置１０に対して更新要求に対する応答として結果通知を返す。

以上がこの実施形態におけるクライアント装置のルート鍵証明書記憶処理である。

【０１２６】

以下、図１９に処理１３としてクライアント装置の公開鍵証明書記憶処理を、図２０に処理１４としてサーバ装置の公開鍵証明書記憶処理を、図２１に処理１５としてサーバ装置のルート鍵証明書書き換え処理を、図２２に処理１６としてクライアント装置のルート鍵証明書書き換え処理をそれぞれ示すが、これらは、第１の実施形態で図９乃至図１２を用いてそれぞれ説明した処理３乃至処理６と同じ目的の処理であり、証明書管理装置１０と直接通信する装置がクライアント装置４０であることに伴って、処理１１及び処理１２の場合と同様に通信手順を若干変更したのみである。そこで、これらの処理についての説明は省略する。

【０１２７】

また、以上の図１７乃至図２２に示した各処理及び図６に示した処理Ｓの実行タイミングは、証明書管理装置１０の証明書更新部２４が図２３に示すフローチャートに従って管理する。すなわち、ルート鍵の更新を行う場合には、まず図６に示した処理Ｓを実行し、その後処理１１乃至処理１６を実行する。

図２３の記載から明らかなように、この第２の実施形態におけるルート鍵更新処理は、図１３に示した第１の実施形態の場合と対応する処理を、同様な順序で行うものである。そして、このことによる効果も、第１の実施形態の場合と同様である。

【０１２８】

すなわち、この第２の実施形態のデジタル証明書管理システムにおいては、ルート鍵更新処理をこのような手順で行うことにより、証明書管理装置１０がクライアント・サーバシステムを構成する装置のうちクライアント装置４０のみと通信可能な場合でも、第１の実施形態の場合と同様に、サーバ装置３０とクライアント装置４０との間の認証処理に大きな影響を与えることなくルート鍵を自動制御で更新することができる。従って、このようなデジタル証明書管理システムを用いることにより、ルート鍵更新用の特別な通信経路を用意せずにルート鍵を更新することができるので、通信に際してＳＳＬによる認証処理を行うクライアント・サーバシステムを、低コストで運用することができる。

また、この実施形態においては、クライアント装置４０にサーバ機能部４４を設ける必要はあるが、ルート鍵更新処理の手順に通信要求待ちを必要とする箇所がないため、処理を速やかに進め、短期間で完了させることができる。

【０１２９】

〔第３の実施形態：図２４乃至図２７〕

次に、この発明によるデジタル証明書管理装置である証明書管理装置と、クライアント・サーバシステムを構成するクライアント装置及びサーバ装置とによって構成される、この発明のデジタル証明書管理システムの第３の実施形態の構成について説明する。

このデジタル証明書管理システムは、ルート鍵更新処理の内容が第１の実施形態のデジタル証明書管理システムと異なるのみであり、装置の構成は第１の実施形態のものと同様であるのでその説明は省略する。

【０１３０】

このデジタル証明書管理システムにおけるルート鍵証明書の更新動作は、この発明のデ

ジタル証明書管理方法の第３の実施形態に係る動作であり、図２４乃至図２７のシーケンス図に示す処理を、この順で実行するものである。以下の各図に示す処理は、証明書管理装置１０，サーバ装置３０，クライアント装置４０の各ＣＰＵが、所要の制御プログラムを実行することによって行うものである。

このデジタル証明書管理システムの証明書管理装置１０は、ルート鍵証明書の更新事由を検出すると、図２４のシーケンス図に示す処理を開始する。

【０１３１】

図２４に示す処理は、第１の実施形態の説明において図６に示した処理Ｓと対応する処理Ｔである。そして、まずステップＳ３０１及びＳ３０２において、図６のステップＳ１０１及びＳ１０２の場合と同様に、有効なルート私有鍵について、新たなルート私有鍵とルート鍵のペアを作成すると共に、その新ルート鍵に従前のルート私有鍵を用いたデジタル署名を付し、第１の証明鍵証明書である配布用ルート鍵証明書を作成する。

そしてさらに、ステップＳ３０３において、図１１のステップＳ１５１の場合と同様に、新ルート鍵に新ルート私有鍵を用いたデジタル署名を付して第２の証明鍵証明書として新ルート鍵証明書を作成する。

【０１３２】

その後、続いて図２５のシーケンス図に示す処理２１を行う。この処理は、第１の実施形態の説明において図８に示した処理２及び図９に示した処理３を併せ、さらに図１２に示した処理６の一部を加えた処理に相当する。

ここではまず、ステップＳ３１１で、図９のステップＳ１３１の場合と同様に、証明書管理装置１０がクライアント公開鍵に新ルート私有鍵を用いたデジタル署名を付して新クライアント公開鍵証明書を作成する。

【０１３３】

そしてステップＳ３１２で、証明書管理装置１０がサーバ装置３０に対して、図２４のステップＳ３０２で作成した配布用ルート鍵証明書と、図２４のステップＳ３０３で作成した新ルート鍵証明書と、ステップＳ３１１で作成した新クライアント公開鍵証明書と共に、これらについての更新要求をクライアント装置４０に送信するよう要求する更新要求送信要求を送信する。サーバ装置３０はこれに応じて、図８のステップＳ１２２及びＳ１２３の場合と同様に、クライアント装置４０からの通信要求（Ｓ３１３）に対する応答としてこれらの証明書とそれらについての更新要求とを送信するようにしている（Ｓ３１４）。

以上の処理により、証明書管理装置１０からクライアント装置４０にサーバ装置３０を介して上記の各証明書とそれらについての更新要求とが送信されることになり、ステップＳ３１２の処理においては、証明書管理装置１０のＣＰＵ１１が第１の送信手段として機能する。

【０１３４】

クライアント装置４０は、この要求を受け取ると、ステップＳ３１５及びＳ３１６で、図８のステップＳ１２４及びＳ１２５の場合と同様に、従前のルート鍵証明書を用いて配布用ルート鍵証明書の正当性を確認し、これが確認できると配布用ルート鍵証明書を証明書記憶部４１に記憶する。このとき、まだ従前のルート鍵証明書は消去しない。

そしてさらにステップＳ３１７で、図１２のステップＳ１６５の場合と同様に、記憶した配布用ルート鍵証明書を用いて新ルート鍵証明書の正当性を確認する。そして、これが確認できると、次のステップＳ３１８で新ルート鍵証明書を証明書記憶部４１に記憶する。この時点で配布用ルート鍵は消去してしまってもよいが、ここでは記憶したままとする。

これらのステップＳ３１５乃至Ｓ３１８の処理において、クライアント装置４０のＣＰＵが第２のクライアント側更新手段として機能する。

【０１３５】

次に、ステップＳ３１９及びＳ３２０で、図９のステップＳ１３５及びＳ１３６の場合と同様に、新クライアント公開鍵証明書の正当性を確認し、これが確認できると、新クラ

イアント公開鍵証明書を証明書記憶部４１に記憶する。ただし、ここでは既に新ルート鍵証明書を記憶しているので、新クライアント公開鍵証明書の正当性は、配布用ルート鍵証明書ではなく新ルート鍵証明書を用いて確認することができる。これらのステップＳ３１９及びＳ３２０において、クライアント装置４０のＣＰＵが第１のクライアント側更新手段として機能する。

【０１３６】

このとき、まだ従前のクライアント公開鍵証明書は消去しない。従って、証明書記憶部４１には２つのクライアント公開鍵証明書が記憶された状態となる。この状態で通信相手に対して公開鍵証明書を送信する場合には、まず新公開鍵証明書を送信するものとする。ここではまだサーバ装置３０に新ルート鍵を記憶させていないので、サーバ装置３０は新公開鍵証明書のデジタル署名を復号化できず、認証が失敗した旨の応答を受けることになる。しかしこの場合でも、再度通信を要求し、この際に従前の公開鍵証明書を送信すれば、従前のルート鍵によってそこに付されたデジタル署名を復号化できるので、問題なく認証を受けることができる。

【０１３７】

なお、ステップＳ３１９及びＳ３２０の処理を、ステップＳ３１７及びＳ３１８の処理より前に行うようにしてもよい。この場合には、ステップＳ３１９における正当性の確認は、配布用ルート鍵証明書を用いて行うことになる。

クライアント装置４０はその後、ステップＳ３２１で、証明書管理装置１０に対して更新要求に対する応答として結果通知を返すが、これはまずサーバ装置３０に対して送信し、サーバ装置３０がステップＳ３２２で証明書管理装置１０に対して送信する。

【０１３８】

その後、続いて図２６のシーケンス図に示す処理２２を行う。この処理は、第１の実施形態の説明において図７に示した処理１及び図１０に示した処理４を併せ、さらに図１１に示した処理５の一部を加えた処理に相当する。

ここではまず、ステップＳ３２３で、図１０のステップＳ１４１の場合と同様に、証明書管理装置１０がサーバ公開鍵に新ルート私有鍵を用いたデジタル署名を付して新サーバ公開鍵証明書を作成する。

【０１３９】

そして、ステップＳ３２４で、証明書管理装置１０がサーバ装置３０に対して、図２４のステップＳ３０２で作成した配布用ルート鍵証明書と、図２４のステップＳ３０３で作成した新ルート鍵証明書と、ステップＳ３２３で作成した新サーバ公開鍵証明書と共に、これらについての更新要求を送信する。このステップＳ３２４の処理においては、証明書管理装置１０のＣＰＵ１１が第２の送信手段として機能する。

サーバ装置３０は、この要求を受け取ると、ステップＳ３２５及びＳ３２６で、図７のステップＳ１１２及びＳ１１３の場合と同様に、従前のルート鍵証明書を用いて配布用ルート鍵証明書の正当性を確認し、これが確認できると配布用ルート鍵証明書を証明書記憶部３１に記憶する。このとき、まだ従前のルート鍵証明書は消去しない。

【０１４０】

そしてさらにステップＳ３２７で、図１１のステップＳ１５３の場合と同様に、記憶した配布用ルート鍵証明書を用いて新ルート鍵証明書の正当性を確認する。そして、これが確認できると、次のステップＳ３２８で新ルート鍵証明書を証明書記憶部３１に記憶すると共に、配布用ルート鍵証明書と従前のルート鍵証明書を廃棄する。この時点では既にクライアント装置４０に新クライアント公開鍵証明書を記憶させてあるので、従前のルート鍵は不要であり、改めて廃棄要求を行うよりもここで廃棄してしまった方が処理の手順が簡単になるので、このようにしたものである。もちろん、改めて廃棄要求を行うようにしてもよい。

これらのステップＳ３２４乃至Ｓ３２８において、サーバ装置３０のＣＰＵが第２のサーバ側更新手段として機能する。

【０１４１】

次に、ステップＳ３２９及びＳ３３０で、図１０のステップＳ１４３及びＳ１４４の場合と同様に、新サーバ公開鍵証明書の正当性を確認し、これが確認できると、新サーバ公開鍵証明書を証明書記憶部３１に記憶し、従前のサーバ公開鍵証明書と置き換える。ただし、ここでは既に新ルート鍵証明書を記憶しているので、新クライアント公開鍵証明書の正当性は、配布用ルート鍵証明書ではなく新ルート鍵証明書を用いて確認することができる。これらのステップＳ３２９及びＳ３３０において、サーバ装置３０のＣＰＵが第１のサーバ側更新手段として機能する。

【０１４２】

このとき従前のサーバ公開鍵証明書を消去する理由は、第１の実施形態において図９の説明で述べた通りである。そして、ステップＳ３３０の時点では既にクライアント装置に新ルート鍵を記憶させてあるので、新サーバ公開鍵証明書を記憶させておけば、認証処理には全く問題ない。

なお、ステップＳ３２９及びＳ３３０の処理を、ステップＳ３２７及びＳ３２８の処理より前に行うようにしてもよい。この場合には、ステップＳ３２９における正当性の確認は、配布用ルート鍵証明書を用いて行うことになる。

【０１４３】

サーバ装置３０はその後、ステップＳ３３１で証明書管理装置１０に対して更新要求に対する応答として結果通知を返す。

以上の図２６に示す処理により、サーバ装置３０側ではルート鍵更新処理が完了する。

【０１４４】

その後、続いて図２７のシーケンス図に示す処理２３を行う。

ここではまずステップＳ３３２で、証明書管理装置１０がサーバ装置３０に対して、不要になったデジタル証明書の廃棄を求める旧鍵廃棄要求をクライアント装置４０に送信するよう要求する旧鍵廃棄要求送信要求を送信する。サーバ装置３０は、これに応じて、クライアント装置４０からの通信要求（Ｓ３３３）に対する応答として旧鍵廃棄要求を送信するようにしている（Ｓ３３４）。

以上の処理により、証明書管理装置１０からクライアント装置４０にサーバ装置３０を介して上記の旧鍵廃棄要求が送信されることになる。

【０１４５】

クライアント装置４０は、この要求を受け取ると、ステップＳ３３５で、証明書記憶部４１に記憶している配布用ルート鍵証明書、従前のルート鍵証明書、および従前のクライアント公開鍵証明書を廃棄する。この時点では、サーバ装置３０に新ルート鍵証明書及び新サーバ公開鍵証明書が記憶されているので、これらの証明書を消去しても認証処理に影響はない。

クライアント装置４０はその後、ステップＳ３３６で証明書管理装置１０に対して更新要求に対する応答として結果通知を返すが、これはまずサーバ装置３０に対して送信し、サーバ装置３０がステップＳ３３７で証明書管理装置１０に対して送信する。

以上により、ルート鍵更新処理を終了する。

【０１４６】

このデジタル証明書管理システムにおいても、ルート鍵更新処理をこのような手順で行うことにより、第１の実施形態の場合と同様に、サーバ装置３０とクライアント装置４０との間の認証処理に大きな影響を与えることなく、ルート鍵を自動制御で更新することができる。従って、このようなデジタル証明書管理システムを用いることにより、ルート鍵更新用の特別な通信経路を用意せずにルート鍵を更新することができるので、通信に際してＳＳＬによる認証処理を行うクライアント・サーバシステムを、低コストで運用することができる。

【０１４７】

なお、この実施形態では、サーバ装置３０に新ルート鍵を記憶させる前にクライアント装置４０に新クライアント公開鍵証明書を記憶させるので、サーバ装置３０に新ルート鍵を記憶させるまでは、通信に、新クライアント公開鍵証明書のデジタル署名をサーバ装置

３０が復号化できないことによるオーバーヘッドが生じる。しかし一方で、証明書管理装置１０からサーバ装置３０（あるいはサーバ装置３０を介してクライアント装置４０）に計３回の要求を送信するのみでルート鍵の更新処理を行うことができる。従って、６回の要求送信が必要な第１の実施形態の場合と比較して、処理手順の管理やプログラムの設計が容易であるという効果がある。ルート鍵証明書を更新すべきサーバ装置やクライアント装置の数が多い場合には、この効果はより大きくなり、この実施形態が有効である。

また、処理２１や処理２２において、各証明書について正当性を確認した後で必要なものを一括して記憶するようにすれば、証明書を記憶する不揮発メモリへのアクセス回数を低減し、処理負荷を低減すると共に処理を高速化することができる。

【０１４８】

〔第４の実施形態：図２４，図２８乃至図３０〕

次に、この発明によるデジタル証明書管理装置である証明書管理装置と、クライアント・サーバシステムを構成するクライアント装置及びサーバ装置とによって構成される、この発明のデジタル証明書管理システムの第４の実施形態の構成について説明する。

このデジタル証明書管理システムは、ルート鍵更新処理の内容が第２の実施形態のデジタル証明書管理システムと異なるのみであり、装置の構成は第２の実施形態のものと同様であるのでその説明は省略する。

【０１４９】

このデジタル証明書管理システムにおけるルート鍵証明書の更新動作は、この発明のデジタル証明書管理方法の第４の実施形態に係る動作であり、図２４及び図２８乃至図３０のシーケンス図に示す処理Ｔ及び処理３１乃至３３を、この順で実行するものである。以下の各図に示す処理は、証明書管理装置１０，サーバ装置３０，クライアント装置４０の各ＣＰＵが、所要の制御プログラムを実行することによって行うものである。

【０１５０】

また、これらの処理は、図２４に示す部分については第３の実施形態の場合と共通であり、図２８乃至図３０に示す部分については、第３の実施形態で図２５乃至図２７を用いてそれぞれ説明した処理と同じ目的の処理であり、証明書管理装置１０と直接通信する装置がクライアント装置４０であることに伴って、第２の実施形態で図１７及び図１８を用いて説明した処理１１及び処理１２の場合と同様に通信手順を若干変更したのみである。そこで、これらの処理についての詳細な説明は省略する。

【０１５１】

そして、この第４の実施形態のデジタル証明書管理システムにおいても、ルート鍵更新処理をこのような手順で行うことにより、証明書管理装置１０がクライアント・サーバシステムを構成する装置のうちクライアント装置４０のみと通信可能な場合でも、第３の実施形態の場合と同様に、サーバ装置３０とクライアント装置４０との間の認証処理に大きな影響を与えることなくルート鍵を自動制御で更新することができる。従って、このようなデジタル証明書管理システムを用いることにより、ルート鍵更新用の特別な通信経路を用意せずにルート鍵を更新することができるので、通信に際してＳＳＬによる認証処理を行うクライアント・サーバシステムを、低コストで運用することができる。また、処理手順の管理やプログラムの設計が容易であるという効果もある。

【０１５２】

〔変形例〕

以上説明した実施形態では、クライアント装置４０とサーバ装置３０とが図４や図５を用いて説明したようなＳＳＬによる認証処理を行う場合の例について説明した。しかし、この認証処理が必ずしもこのようなものでなくてもこの発明は効果を発揮する。

ＳＳＬを改良したＴＬＳ（Transport Layer Security）も知られているが、このプロトコルに基づく認証処理を行う場合にも当然適用可能である。

【０１５３】

また、上述した実施形態では、証明書管理装置１０をサーバ装置３０あるいはクライアント装置４０とは別に設ける例について説明したが、サーバ装置３０あるいはクライアン

ト装置４０と一体として設けることを妨げるものではない。この場合、証明書管理装置１０の機能を実現するためのＣＰＵ，ＲＯＭ，ＲＡＭ等の部品を独立して設けてもよいが、ハードウェア資源としてはサーバ装置３０あるいはクライアント装置４０のＣＰＵ，ＲＯＭ，ＲＡＭ等を使用し、そのＣＰＵに適当なソフトウェアを実行させることにより、証明書管理装置１０として機能させるようにしてもよい。

【０１５４】

このような場合において、証明書管理装置１０と、これと一体になっているサーバ装置３０あるいはクライアント装置４０との間の通信には、ハードウェアを証明書管理装置１０として機能させるためのプロセスと、ハードウェアをサーバ装置３０あるいはクライアント装置４０として機能させるためのプロセスとの間のプロセス間通信を含むものとする。

さらに、上述した各実施形態では、証明書管理装置１０が証明鍵やデジタル証明書を自ら作成してこれを取得する例について説明したが、図２及び図１６に示した証明用鍵作成部２１や証明書発行部２２の機能を証明書管理装置１０とは別の装置に設け、証明書管理装置１０がその装置から証明鍵やデジタル証明書の供給を受けてこれらを取得するようにしてもよい。

【０１５５】

また、証明書管理装置１０がサーバ装置３０及びクライアント装置４０の双方と直接的に通信が可能な構成としても構わない。この場合、図７乃至図１２等に示した通信シーケンスは、双方の装置と直接通信が可能であることに伴って異なったものになるが、処理の順序は上述した各実施形態の場合と同様である。このようにしても、上述した各実施形態の効果を得ることができる。

【０１５６】

また、上述したように、第２及び第４の実施形態においては、証明書管理装置１０とクライアント装置４０との間で通信を行う際にも、ＳＳＬによる認証処理を行うようにすることができる。

このようにするには、図３１に示すように、クライアント装置４０に、サーバ装置３０との間の認証処理に用いるクライアント私有鍵、クライアント公開鍵証明書及びルート鍵証明書（実施形態において説明したもの）とは別に、もう一組の私有鍵、公開鍵証明書及びルート鍵証明書（「第２のクライアント私有鍵」、「第２のクライアント公開鍵証明書」及び「第２のルート鍵証明書」と呼ぶ）を記憶させ、証明書管理装置１０との間の認証処理にこれらを用いるようにすればよい。

【０１５７】

この場合、証明書管理装置１０にも、管理装置用私有鍵、管理装置用公開鍵証明書及び上記の第２のルート鍵証明書を記憶させ、認証処理に用いる。そして、第２のクライアント公開鍵証明書及び管理装置用公開鍵証明書は、第２のルート鍵証明書に含まれる第２のルート鍵で内容が確認できるものとする。すなわち、その第２のルート鍵と対応するルート私有鍵（第２のルート私有鍵）を用いてデジタル署名を付すようにする。

このようにすれば、証明書管理装置１０とクライアント装置４０との間の認証処理と、クライアント装置４０とサーバ装置３０との間の認証処理とを、全く独立して行うことができる。

【０１５８】

第２及び第４の実施形態におけるクライアント装置４０は、図１６を用いて説明したように、証明書管理装置１０との通信はサーバ機能部４４が、サーバ装置３０との通信はクライアント機能部４３が通信機能部４２を介して行う。従って、証明書管理装置１０から通信を要求される通信と、サーバ装置３０に要求する通信とは明確に区別することができるため、これらとの間で別々の鍵や証明書を用いた認証処理を行うことができるのである。

このような場合において、証明書管理装置１０からの要求に応じてクライアント装置４０とサーバ装置３０との間の認証処理に用いるルート鍵証明書や公開鍵証明書を更新した

としても、証明書管理装置１０とクライアント装置４０との間の認証処理には全く影響がない。

【０１５９】

各実施形態で説明した手順によって更新処理を行えば、クライアント装置４０とサーバ装置３０との間の認証処理にも大きな影響を与えることなく更新処理を行えることは上述した通りであるので、図３１に示した構成をとることにより、各ノード間の認証処理を維持したままルート鍵を更新できると言える。

なお、第２のルート鍵証明書を更新しようとする場合には、証明書管理装置１０をクライアント、クライアント装置４０をサーバとして、上述したいずれかの実施形態の手順に従って更新処理を行えばよい。このような更新処理を行っても、クライアント装置４０とサーバ装置３０との間の認証処理には全く影響がない。

【０１６０】

また、上述した各実施形態においては、クライアント装置４０とサーバ装置３０とが相互認証を行う際に必要な、クライアント装置４０とサーバ装置３０の双方に記憶させているルート鍵証明書及び公開鍵証明書を更新する例について説明した。しかし、図５を用いて説明したように、クライアント装置４０がサーバ装置３０を認証するのみでよいのであれば、クライアント装置４０に公開鍵証明書を、サーバ装置３０にルート鍵証明書を記憶させておけば足りる。従って、更新についてもこれらのみを更新すれば足りる。

そこで、例えば第１の実施形態に示したルート鍵証明書の更新処理を、以下のように簡略化することができる。すなわち、図３４に示すように、図６に示したルート鍵証明書作成処理（処理Ｓ）、図８に示したクライアント装置のルート鍵証明書記憶処理（処理２）、図３２に示すサーバ装置の公開鍵証明書記憶処理（処理２４）、図３３に示すクライアント装置のルート鍵証明書書き換え処理（処理２６）を、この順番で実行するようにすればよい。

【０１６１】

これらの処理において、処理２４は、図１０に示した処理４と対応するものであるが、サーバ装置３０にルート鍵証明書を記憶させない場合には、ステップＳ１４４では、証明書管理装置１０から受信した新サーバ公開鍵証明書を信用し、そのまま従前のサーバ公開鍵証明書を置き換えるようにしている。また、ステップＳ１４２′で配布用ルート鍵証明書も送信し、これを用いて新サーバ公開鍵証明書の正当性を確認できるようにしてもよい（Ｓ１４３）。このようにする場合、サーバ装置３０側にもクライアント装置４０側と同じルート鍵証明書を記憶させておくようにすれば、それを用いて配布用ルート鍵証明書の正当性を確認することもできる。

また、処理２６は、図１２に示した処理６と対応するものであり、クライアント装置４０側には公開鍵証明書を更新しないことから、ステップＳ１６６′から公開鍵証明書を廃棄する処理を除いた点が、処理６と異なるのみである。

【０１６２】

以上のような処理においても、サーバ装置３０に対して新サーバ公開鍵証明書を送信する動作を、クライアント装置４０から新ルート鍵証明書を受信した旨の情報を受信した後に行うことに変わりはない。そして、このようにすることにより、第１の実施形態の場合と同様に、サーバ装置３０とクライアント装置４０との間の認証処理に大きな影響を与えることなく、ルート鍵を自動制御で更新することができる。

なお、第２乃至第４の実施形態についても同様にこのような変形を適用可能であることは、いうまでもない。

【０１６３】

また、上述した各実施形態においては、クライアント装置４０とサーバ装置３０で共通のルート鍵証明書を用いる例について説明したが、必ずしもこのようにする必要はない。すなわち、図３５に示すように、クライアント装置４０とサーバ装置３０で別々のルート鍵証明書を記憶させるようにしてもよい。このようにしても、サーバ装置３０側でクライアント公開鍵証明書の正当性を確認でき、クライアント装置４０側でサーバ公開鍵証明書

の正当性を確認できれば、認証処理には全く問題ない。

【０１６４】

そして、このような場合には、各ルート鍵証明書を独立して更新することが考えられ、その場合にはそのルート鍵証明書を用いて正当性を確認すべき公開鍵証明書も共に更新することになる。そして、このような処理も、上述した各実施形態の場合と同様な考え方により、クライアント装置４０側に記憶させているルート鍵証明書（サーバルート鍵証明書）の更新が終了した後でサーバ装置３０側に記憶させている公開鍵証明書（サーバ公開鍵証明書）を更新するようにすれば、クライアント装置４０とサーバ装置３０との間の認証処理が可能な状態のまま、ルート鍵を更新することができる。サーバ装置３０側に記憶させているルート鍵証明書（クライアントルート鍵証明書）の更新が終了した後でクライアント装置４０側に記憶させている公開鍵証明書（クライアント公開鍵証明書）を更新するようにするとよいことも、第１の実施形態で説明した場合と同様である。

【０１６５】

この処理の具体例を示すと、例えば、図３６乃至図３９に示す各処理を、図４０に示す順番で実行すればよい。図３６乃至図３９に示す各処理は、それぞれ第１の実施形態で図６に示した処理Ｓ，図８に示した処理２，図１０に示した処理４，図１２に示した処理６に対応するものである。

そして、図３６のステップＳ５０３にて作成した確認用ルート鍵証明書は、サーバ装置３０に新サーバ公開鍵証明書の正当性を確認させるために使用するものである。ここでは、サーバ公開鍵証明書はクライアント用ルート鍵証明書を用いて正当性を確認するものであり、サーバ装置３０は、自身で記憶しているサーバ用ルート鍵証明書ではサーバ公開鍵証明書の正当性を確認できないため、確認用ルート鍵証明書が必要になっている。

なお、このような変形も、第２乃至第４の実施形態に同様に適用可能であることは、いうまでもない。

また、上述の各実施形態及び変形例で説明した技術を相互に組み合わせて用いることも当然可能である。

【０１６６】

また、この発明によるプログラムは、クライアント・サーバシステムを構成する複数の装置とネットワークを介して直接的又は間接的に通信可能なコンピュータに、各機能（証明鍵更新手段，第１の送信手段，第２の送信手段，その他の手段としての機能）を実現させるためのプログラムであり、このようなプログラムをコンピュータに実行させることにより、上述したような効果を得ることができる。

【０１６７】

このようなプログラムは、はじめからコンピュータに備えるＲＯＭあるいはＨＤＤ等の記憶手段に格納しておいてもよいが、記録媒体であるＣＤ－ＲＯＭあるいはフレキシブルディスク，ＳＲＡＭ，ＥＥＰＲＯＭ，メモリカード等の不揮発性記録媒体（メモリ）に記録して提供することもできる。そのメモリに記録されたプログラムをコンピュータにインストールしてＣＰＵに実行させるか、ＣＰＵにそのメモリからこのプログラムを読み出して実行させることにより、上述した各手順を実行させることができる。

さらに、ネットワークに接続され、プログラムを記録した記録媒体を備える外部機器あるいはプログラムを記憶手段に記憶した外部機器からダウンロードして実行させることも可能である。

【産業上の利用可能性】

【０１６８】

以上説明してきた通り、この発明のデジタル証明書管理システム、デジタル証明書管理装置、デジタル証明書管理方法、またはプログラムによれば、クライアント・サーバシステムにおける認証処理でデジタル証明書の正当性を確認するために用いる証明鍵を、更新用の特別な通信経路を設けることなく安全に更新できるようにすることができる。

従って、この発明を、クライアント・サーバシステムにおいて認証処理に使用する証明書の管理に適用することにより、安全に認証用公開鍵の更新が可能なシステムを安価に提

供することができる。

【図面の簡単な説明】

【０１６９】

【図１】この発明のデジタル証明書管理装置の実施形態である証明書管理装置のハードウェア構成を示すブロック図である。

【図２】この発明のデジタル証明書管理システムの第１の実施形態を構成する各装置の、その特徴となる部分の機能構成を示す機能ブロック図である。

【図３】図２に示したデジタル証明書管理システムにおけるデータ送受モデルを示す概念図である。

【図４】クライアント装置とサーバ装置とがＳＳＬによる相互認証を行う際の各装置において実行する処理のフローチャートを、その処理に用いる情報と共に示す図である。

【図５】クライアント装置とサーバ装置とがＳＳＬによる片方向認証を行う際の各装置において実行する処理のフローチャートを、その処理に用いる情報と共に示す図である。

【図６】図２に示したデジタル証明書管理システムにおけるルート鍵更新処理のうち、ルート鍵証明書作成処理を示すシーケンス図である。

【図７】同じくサーバ装置のルート鍵証明書記憶処理を示すシーケンス図である。

【図８】同じくクライアント装置のルート鍵証明書記憶処理を示すシーケンス図である。

【図９】同じくクライアント装置の公開鍵証明書記憶処理を示すシーケンス図である。

【図１０】同じくサーバ装置の公開鍵証明書記憶処理を示すシーケンス図である。

【０１７０】

【図１１】同じくサーバ装置のルート鍵証明書書き換え処理を示すシーケンス図である。

【図１２】同じくクライアント装置のルート鍵証明書書き換え処理を示すシーケンス図である。

【図１３】第１の実施形態のルート鍵更新処理における、図６乃至図１２のシーケンス図に示した各処理の実行順を示すフローチャートである。

【図１４】図７に示したシーケンスの変形例を示す図である。

【図１５】図８に示したシーケンスの変形例を示す図である。

【図１６】この発明のデジタル証明書管理システムの第２の実施形態を構成する各装置の、その特徴となる部分の機能構成を示す機能ブロック図である。

【図１７】図１６に示したデジタル証明書管理システムにおけるルート鍵更新処理のうち、サーバ装置のルート鍵証明書記憶処理を示すシーケンス図である。

【図１８】同じくクライアント装置のルート鍵証明書記憶処理を示すシーケンス図である。

【図１９】同じくクライアント装置の公開鍵証明書記憶処理を示すシーケンス図である。

【図２０】同じくサーバ装置の公開鍵証明書記憶処理を示すシーケンス図である。

【０１７１】

【図２１】同じくサーバ装置のルート鍵証明書書き換え処理を示すシーケンス図である。

【図２２】同じくクライアント装置のルート鍵証明書書き換え処理を示すシーケンス図である。

【図２３】第２の実施形態のルート鍵更新処理における、図６及び図１７乃至図２２のシーケンス図に示した各処理の実行順を示すフローチャートである。

【図２４】この発明のデジタル証明書管理システムの第３の実施形態におけるルート鍵更新処理の一部を示すシーケンス図である。

【図２５】図２４の続きの処理を示すシーケンス図である。
【図２６】図２５の続きの処理を示すシーケンス図である。
【図２７】図２６の続きの処理を示すシーケンス図である。
【図２８】この発明のデジタル証明書管理システムの第４の実施形態におけるルート鍵更新処理の、図２４の続きの処理を示すシーケンス図である。
【図２９】図２８の続きの処理を示すシーケンス図である。
【図３０】図２９の続きの処理を示すシーケンス図である。

【０１７２】

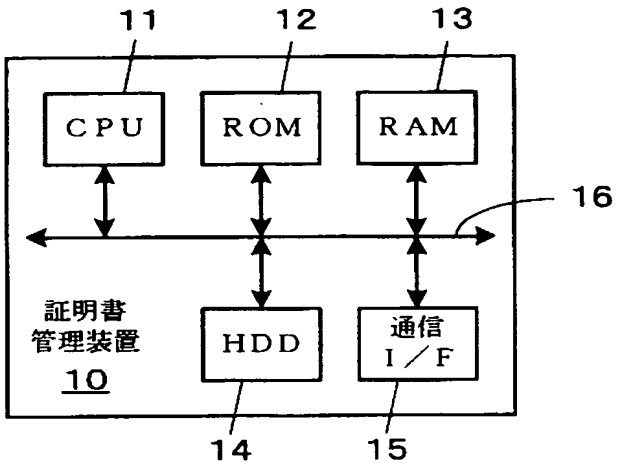
【図３１】この発明のデジタル証明書管理システムの各実施形態の変形例における鍵及び証明書の記憶状態及びその場合のルート鍵更新処理について説明するための図である。
【図３２】各実施形態の変形例におけるサーバ装置の公開鍵証明書記憶処理を示すシーケンス図である。
【図３３】同じくクライアント装置のルート鍵証明書書き換え処理を示すシーケンス図である。
【図３４】同じく各処理の実行順を示すフローチャートである。
【図３５】各実施形態の別の変形例における、鍵及び証明書の記憶状態及びその場合のルート鍵更新処理について説明するための図である。
【図３６】その別の変形例におけるルート鍵証明書作成処理を示すシーケンス図である。
【図３７】同じくクライアント装置のルート鍵証明書記憶処理を示すシーケンス図である。
【図３８】同じくサーバ装置の公開鍵証明書記憶処理を示すシーケンス図である。
【図３９】同じくクライアント装置のルート鍵証明書書き換え処理を示すシーケンス図である。
【図４０】同じく各処理の実行順を示すフローチャートである。
【図４１】公開鍵暗号を用いた認証処理におけるルート鍵、ルート私有鍵、およびサーバ公開鍵の関係について説明するための図である。

【符号の説明】

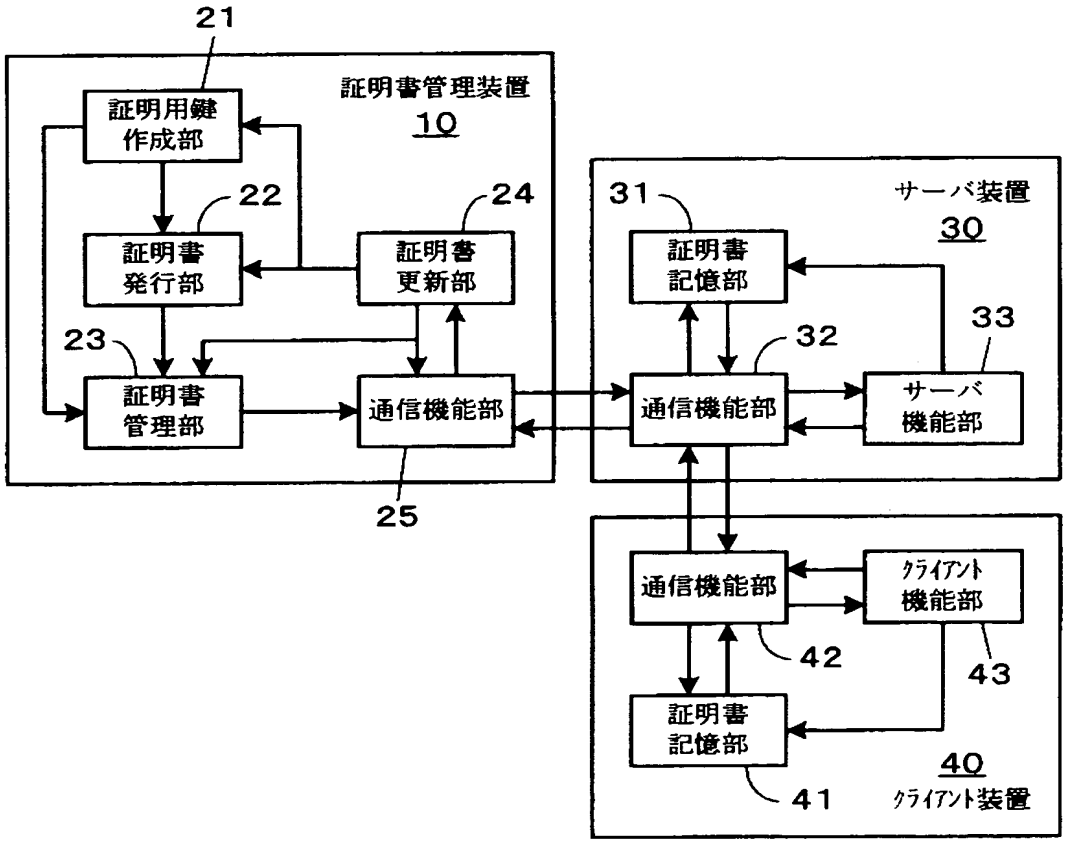
【０１７３】

１０：証明書管理装置　　１１：ＣＰＵ
１２：ＲＯＭ　　１３：ＲＡＭ
１４：ＨＤＤ　　１５：通信Ｉ／Ｆ
１６：システムバス　　２１：証明用鍵作成部
２２：証明書発行部　　２３：証明書管理部
２４：証明書更新部　　２５，３２，４２：通信機能部
３０：サーバ装置　　３１，４１：証明書記憶部
３３，４４：サーバ機能部　　４０：クライアント装置
４３：クライアント機能部

【書類名】図面
【図１】

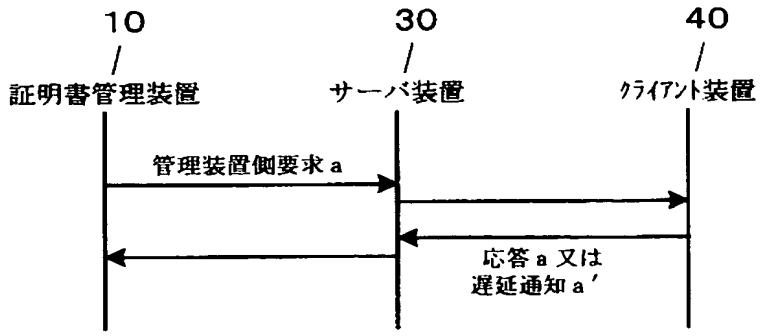

11
12
13
CPU
ROM
RAM
16
証明書
管理装置
10
HDD
通信
I／F
14
15

【図２】

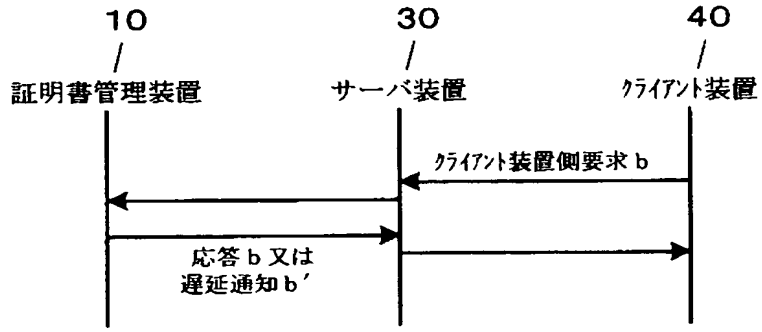

21
証明書管理装置
10
証明用鍵
作成部
22
24
証明書
発行部
証明書
更新部
23
証明書
管理部
通信機能部
25
31
サーバ装置
30
証明書
記憶部
33
32
通信機能部
サーバ
機能部
通信機能部
ｸﾗｲｱﾝﾄ
機能部
42
43
証明書
記憶部
40
41
ｸﾗｲｱﾝﾄ装置

【図３】

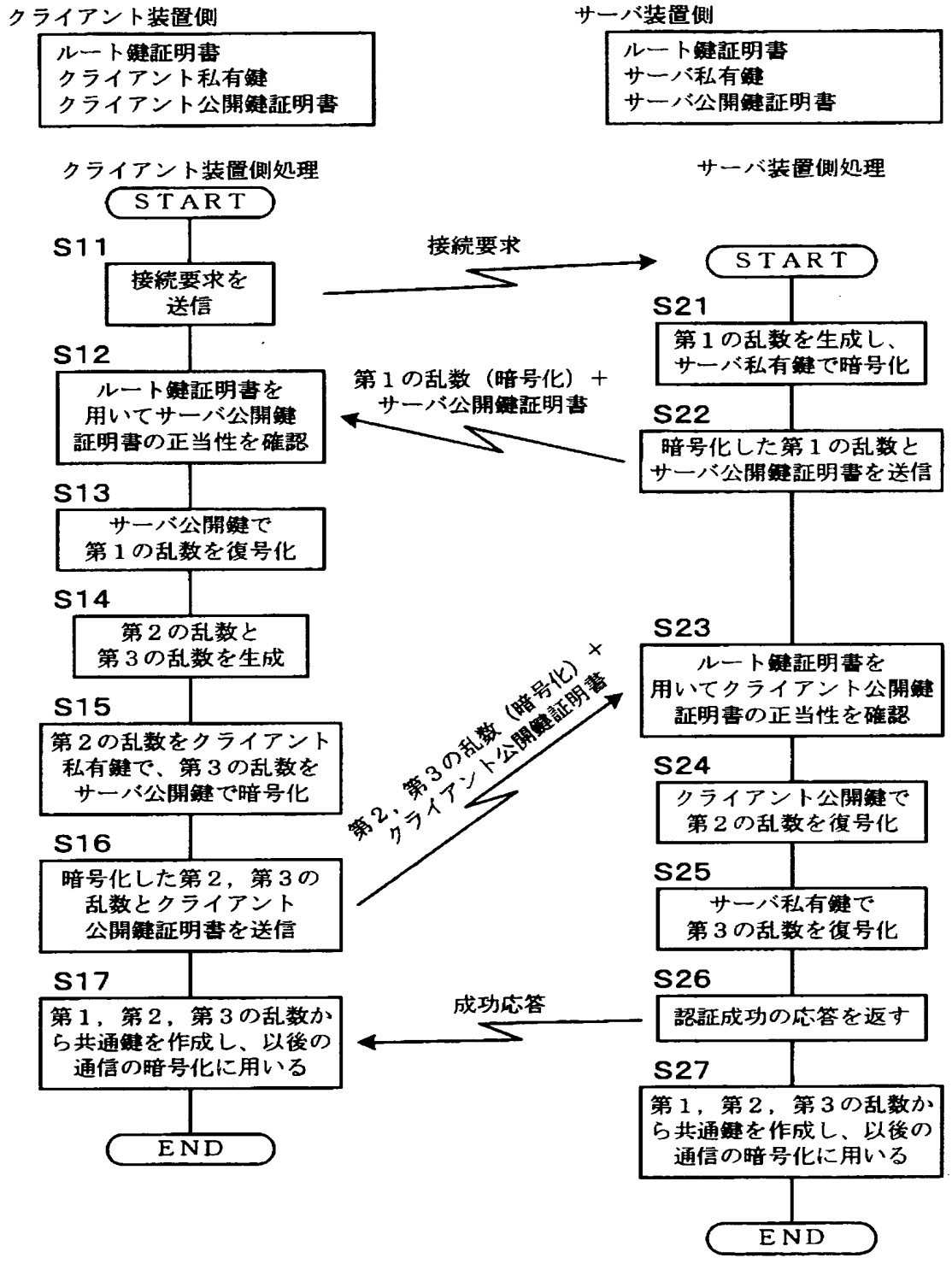
（A）


10
30
40
証明書管理装置
サーバ装置
ｸﾗｲｱﾝﾄ装置
管理装置側要求ａ
応答ａ又は
遅延通知ａ′

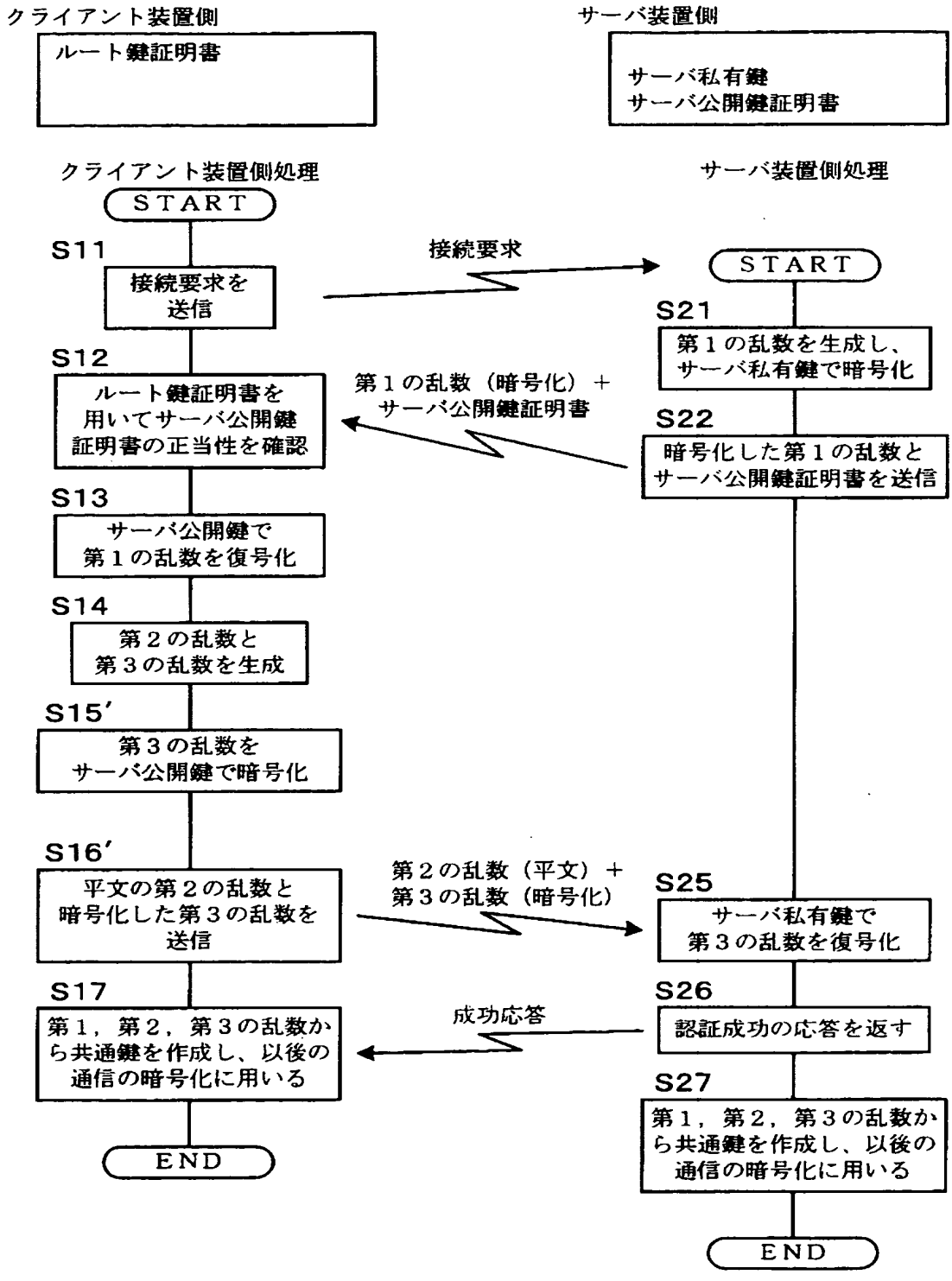
（B）


10
30
40
証明書管理装置
サーバ装置
ｸﾗｲｱﾝﾄ装置
ｸﾗｲｱﾝﾄ装置側要求ｂ
応答ｂ又は
遅延通知ｂ′

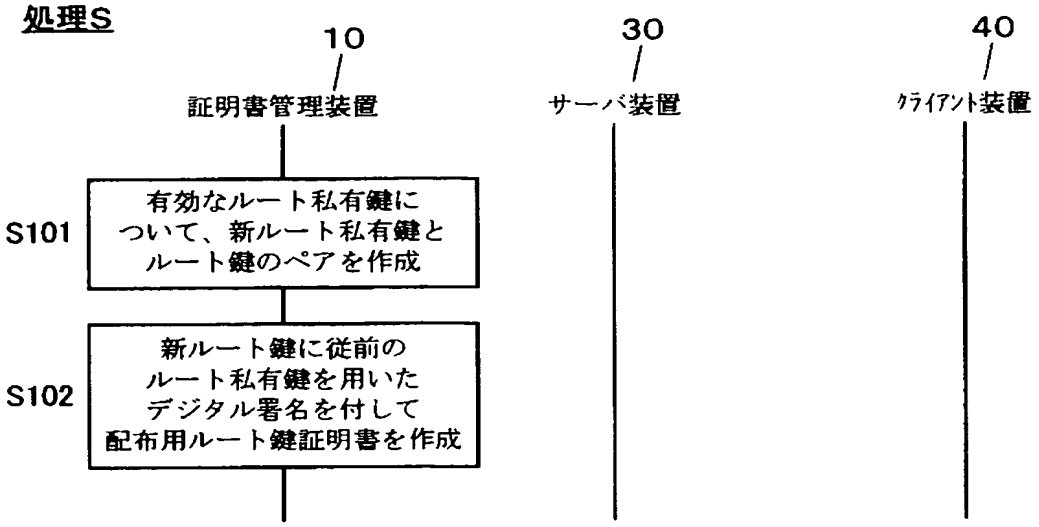
【図４】


クライアント装置側
ルート鍵証明書
クライアント私有鍵
クライアント公開鍵証明書
サーバ装置側
ルート鍵証明書
サーバ私有鍵
サーバ公開鍵証明書
クライアント装置側処理
サーバ装置側処理
START
S11
接続要求を送信
接続要求
START
S21
第１の乱数を生成し、サーバ私有鍵で暗号化
S12
ルート鍵証明書を用いてサーバ公開鍵証明書の正当性を確認
第１の乱数（暗号化）＋サーバ公開鍵証明書
S22
暗号化した第１の乱数とサーバ公開鍵証明書を送信
S13
サーバ公開鍵で第１の乱数を復号化
S14
第２の乱数と第３の乱数を生成
S23
ルート鍵証明書を用いてクライアント公開鍵証明書の正当性を確認
S15
第２の乱数をクライアント私有鍵で、第３の乱数をサーバ公開鍵で暗号化
第２，第３の乱数（暗号化）×クライアント公開鍵証明書
S24
クライアント公開鍵で第２の乱数を復号化
S16
暗号化した第２，第３の乱数とクライアント公開鍵証明書を送信
S25
サーバ私有鍵で第３の乱数を復号化
S17
第１，第２，第３の乱数から共通鍵を作成し、以後の通信の暗号化に用いる
成功応答
S26
認証成功の応答を返す
S27
第１，第２，第３の乱数から共通鍵を作成し、以後の通信の暗号化に用いる
END
END

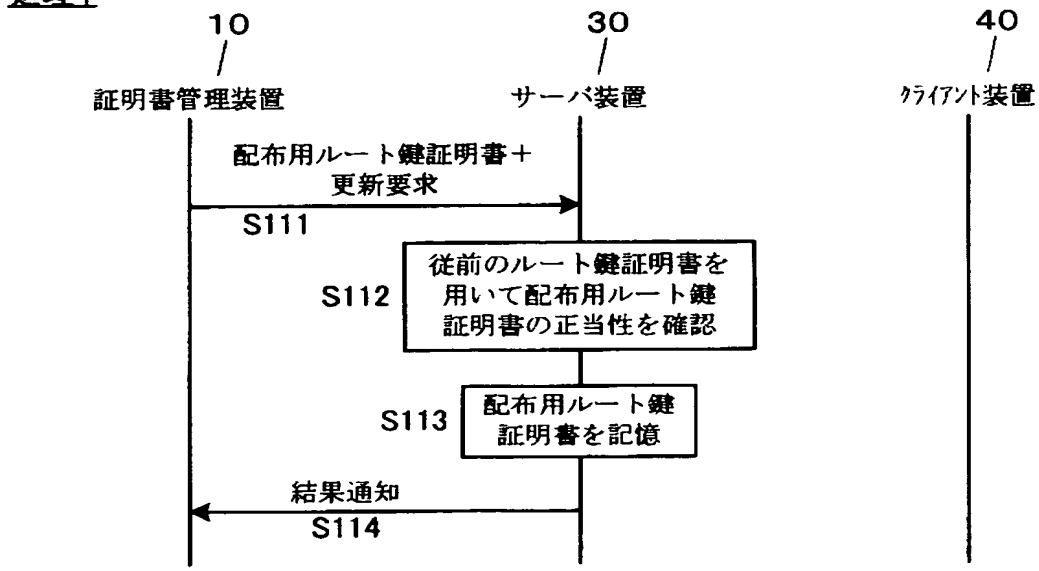
【図５】


クライアント装置側
ルート鍵証明書
サーバ装置側
サーバ私有鍵
サーバ公開鍵証明書
クライアント装置側処理
サーバ装置側処理
START
S11
接続要求を送信
接続要求
START
S21
第１の乱数を生成し、サーバ私有鍵で暗号化
S12
ルート鍵証明書を用いてサーバ公開鍵証明書の正当性を確認
第１の乱数（暗号化）＋サーバ公開鍵証明書
S22
暗号化した第１の乱数とサーバ公開鍵証明書を送信
S13
サーバ公開鍵で第１の乱数を復号化
S14
第２の乱数と第３の乱数を生成
S15′
第３の乱数をサーバ公開鍵で暗号化
S16′
平文の第２の乱数と暗号化した第３の乱数を送信
第２の乱数（平文）＋第３の乱数（暗号化）
S25
サーバ私有鍵で第３の乱数を復号化
S17
第１，第２，第３の乱数から共通鍵を作成し、以後の通信の暗号化に用いる
成功応答
S26
認証成功の応答を返す
S27
第１，第２，第３の乱数から共通鍵を作成し、以後の通信の暗号化に用いる
END
END

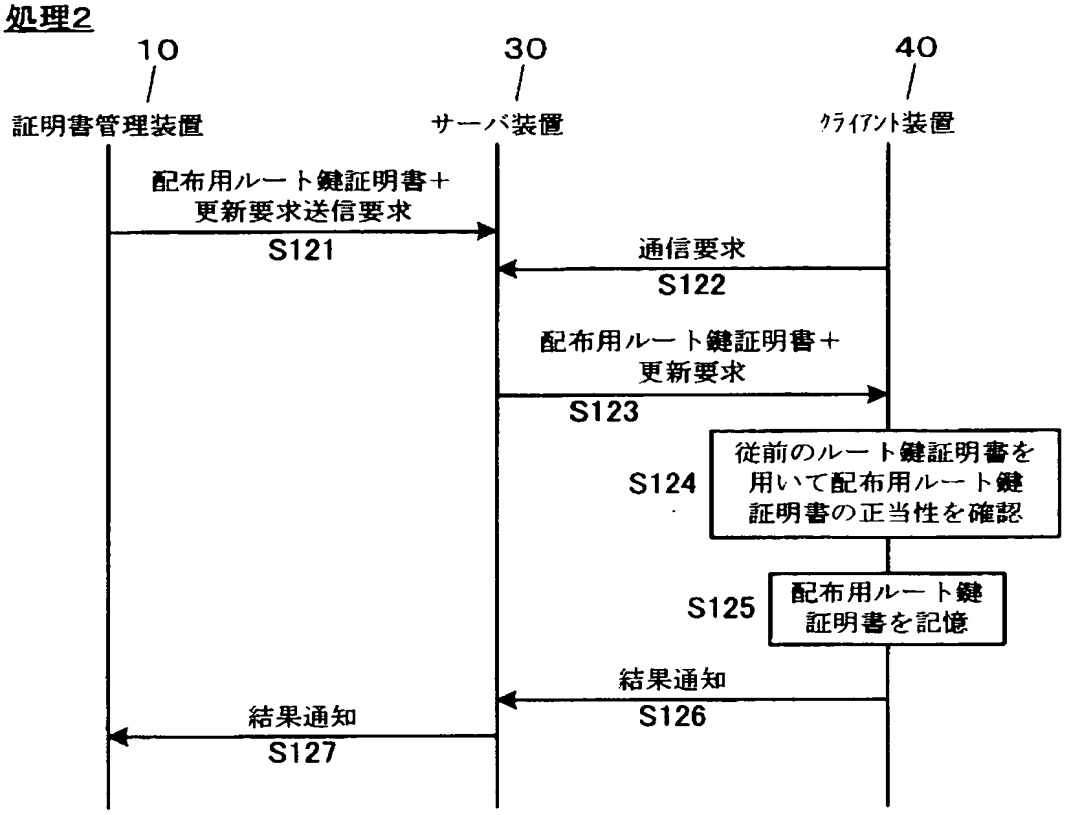
【図６】


処理S
10
証明書管理装置
30
サーバ装置
40
ｸﾗｲｱﾝﾄ装置
S101
有効なルート私有鍵について、新ルート私有鍵とルート鍵のペアを作成
S102
新ルート鍵に従前のルート私有鍵を用いたデジタル署名を付して配布用ルート鍵証明書を作成

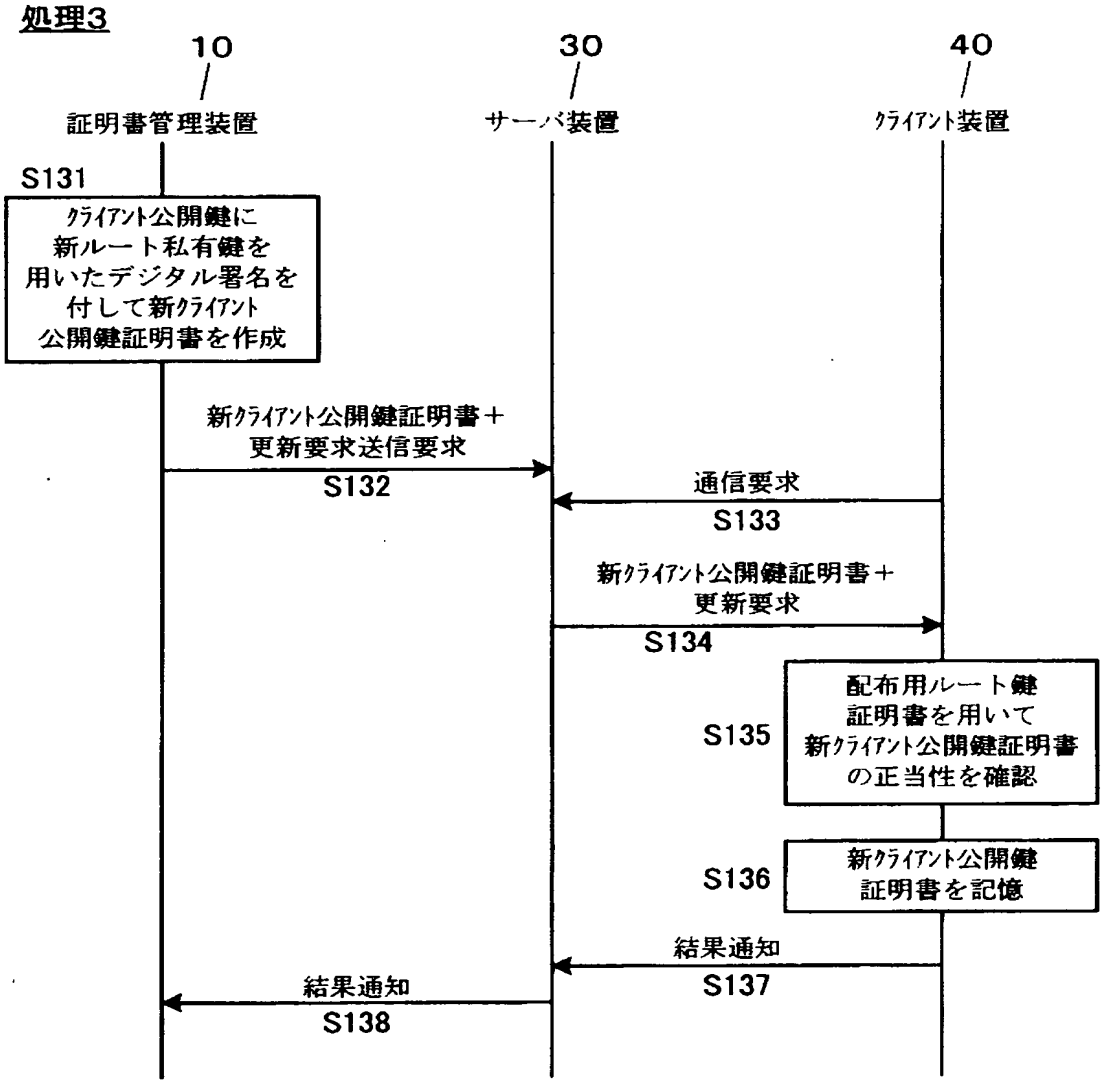
【図７】


処理1
10
証明書管理装置
30
サーバ装置
40
ｸﾗｲｱﾝﾄ装置
配布用ルート鍵証明書＋更新要求
S111
S112
従前のルート鍵証明書を用いて配布用ルート鍵証明書の正当性を確認
S113
配布用ルート鍵証明書を記憶
結果通知
S114

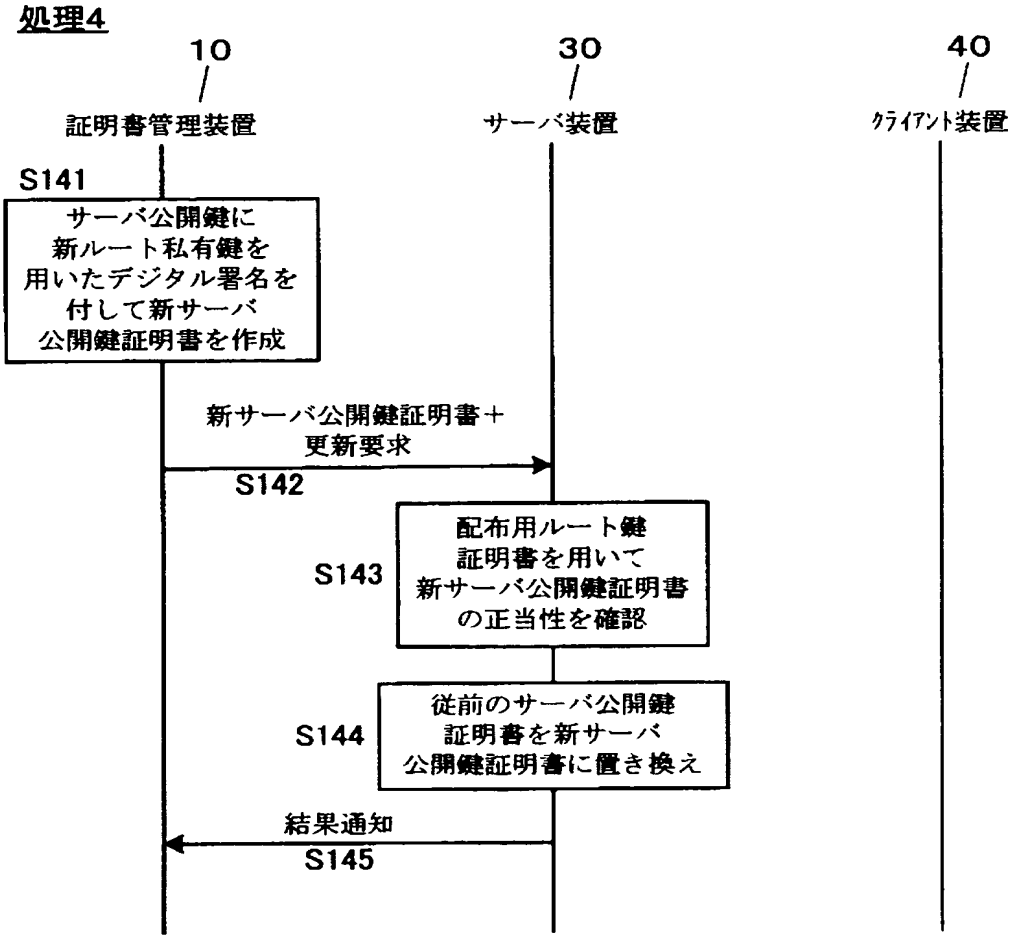
【図８】


処理2
10
30
40
証明書管理装置
サーバ装置
ｸﾗｲｱﾝﾄ装置
配布用ルート鍵証明書＋
更新要求送信要求
S121
通信要求
S122
配布用ルート鍵証明書＋
更新要求
S123
S124
従前のルート鍵証明書を
用いて配布用ルート鍵
証明書の正当性を確認
S125
配布用ルート鍵
証明書を記憶
結果通知
S126
結果通知
S127

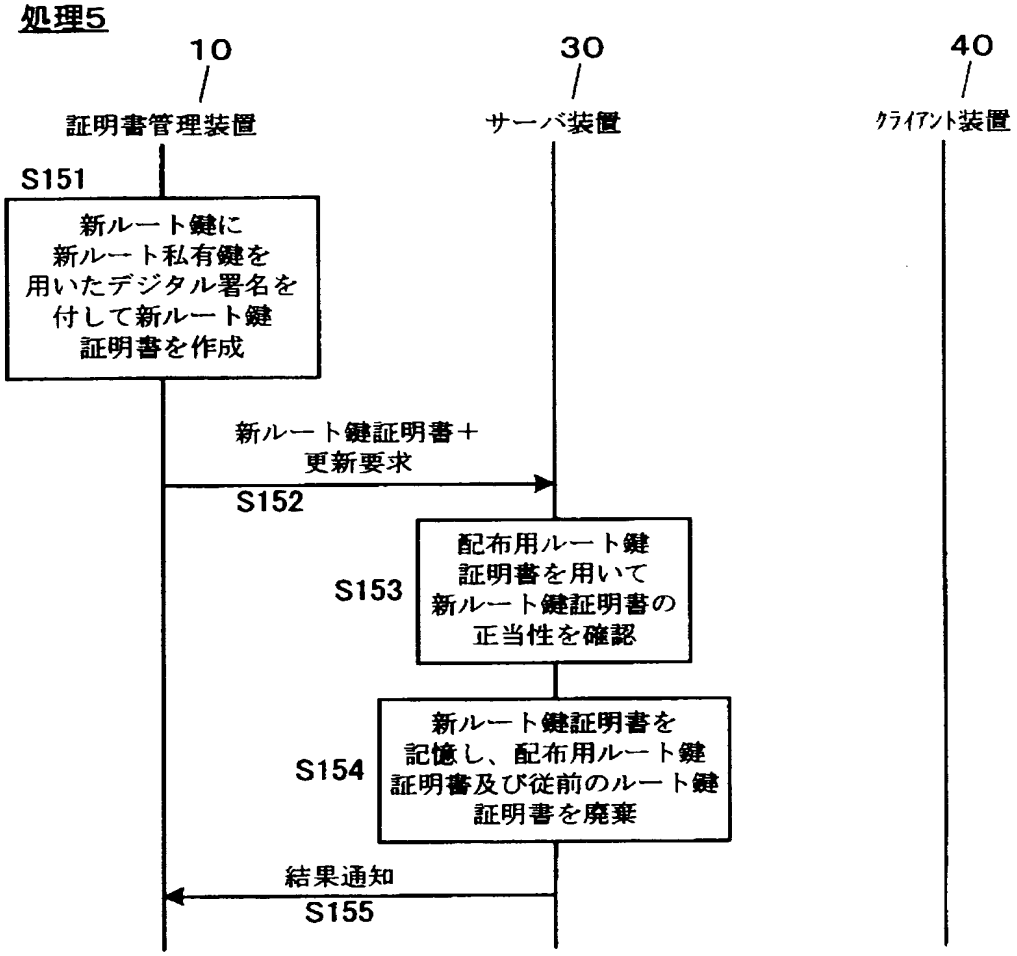
【図９】


処理3
10
30
40
証明書管理装置
サーバ装置
ｸﾗｲｱﾝﾄ装置
S131
ｸﾗｲｱﾝﾄ公開鍵に
新ルート私有鍵を
用いたデジタル署名を
付して新ｸﾗｲｱﾝﾄ
公開鍵証明書を作成
新ｸﾗｲｱﾝﾄ公開鍵証明書＋
更新要求送信要求
S132
通信要求
S133
新ｸﾗｲｱﾝﾄ公開鍵証明書＋
更新要求
S134
S135
配布用ルート鍵
証明書を用いて
新ｸﾗｲｱﾝﾄ公開鍵証明書
の正当性を確認
S136
新ｸﾗｲｱﾝﾄ公開鍵
証明書を記憶
結果通知
S137
結果通知
S138

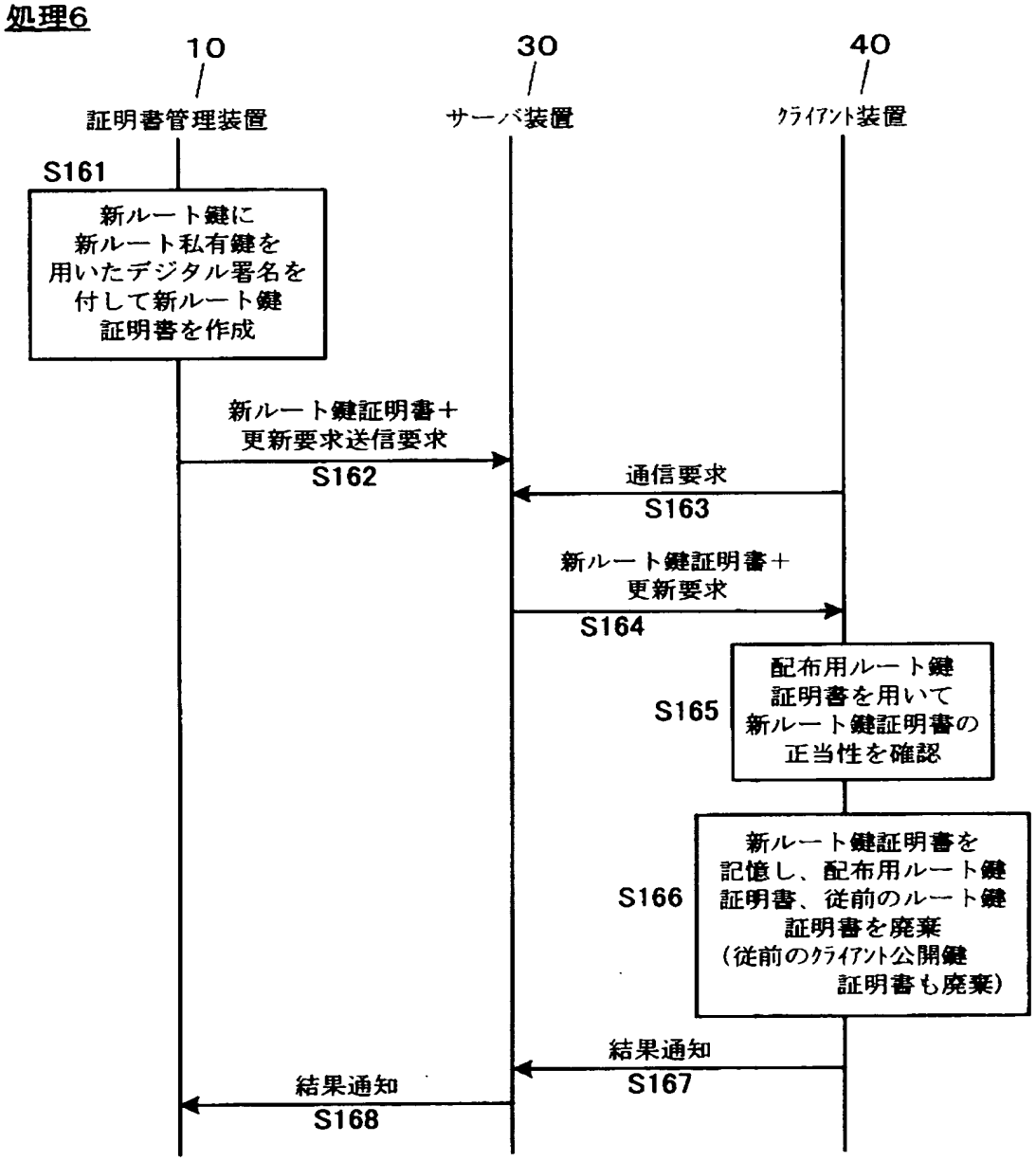
【図１０】


処理4
10
30
40
証明書管理装置
サーバ装置
ｸﾗｲｱﾝﾄ装置
S141
サーバ公開鍵に
新ルート私有鍵を
用いたデジタル署名を
付して新サーバ
公開鍵証明書を作成
新サーバ公開鍵証明書＋
更新要求
S142
S143
配布用ルート鍵
証明書を用いて
新サーバ公開鍵証明書
の正当性を確認
S144
従前のサーバ公開鍵
証明書を新サーバ
公開鍵証明書に置き換え
結果通知
S145

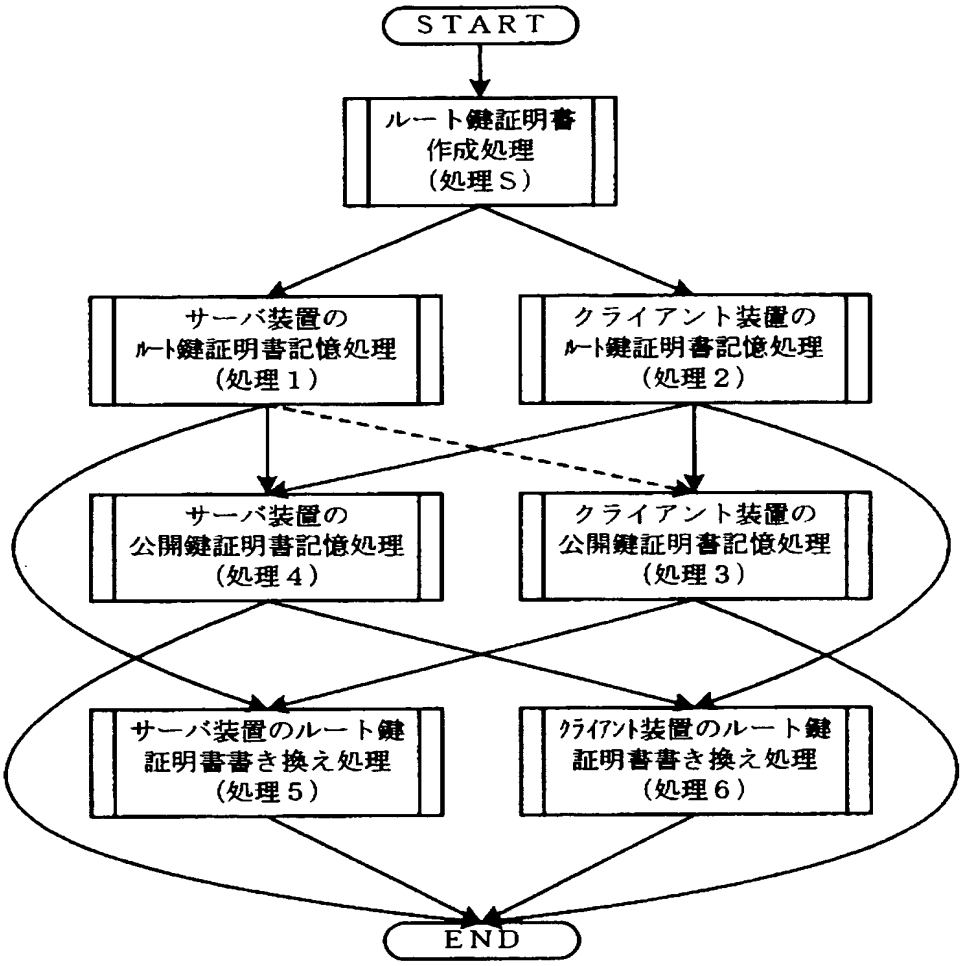
【図１１】


処理5
10
30
40
証明書管理装置
サーバ装置
ｸﾗｲｱﾝﾄ装置
S151
新ルート鍵に
新ルート私有鍵を
用いたデジタル署名を
付して新ルート鍵
証明書を作成
新ルート鍵証明書＋
更新要求
S152
S153
配布用ルート鍵
証明書を用いて
新ルート鍵証明書の
正当性を確認
S154
新ルート鍵証明書を
記憶し、配布用ルート鍵
証明書及び従前のルート鍵
証明書を廃棄
結果通知
S155

【図１２】

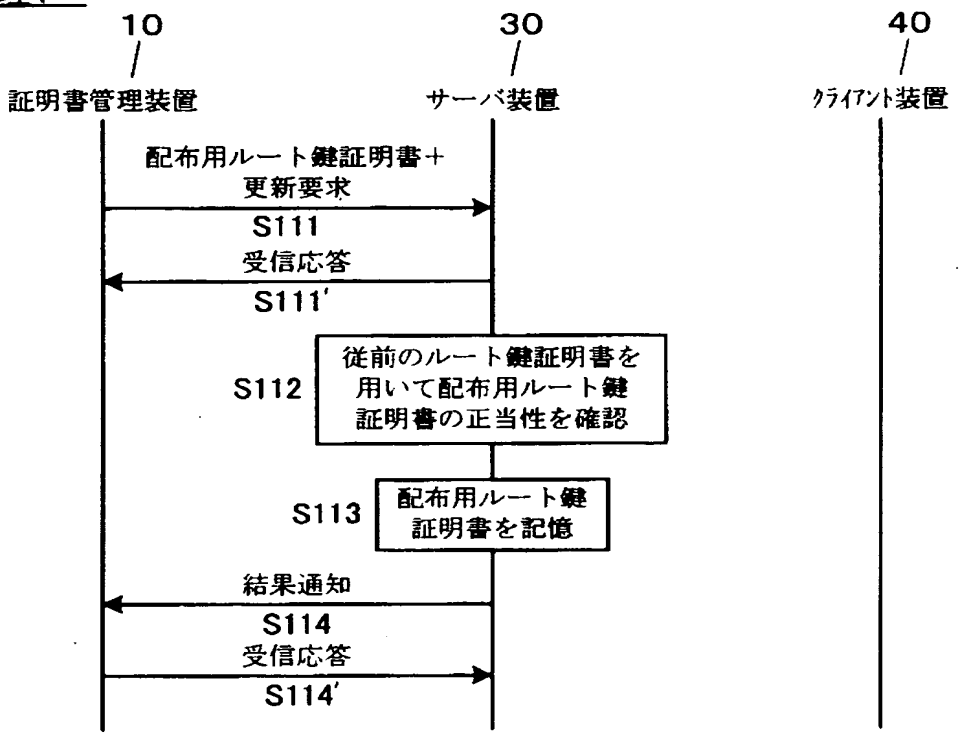

処理6
10
証明書管理装置
30
サーバ装置
40
ｸﾗｲｱﾝﾄ装置
S161
新ルート鍵に
新ルート私有鍵を
用いたデジタル署名を
付して新ルート鍵
証明書を作成
新ルート鍵証明書＋
更新要求送信要求
S162
通信要求
S163
新ルート鍵証明書＋
更新要求
S164
S165
配布用ルート鍵
証明書を用いて
新ルート鍵証明書の
正当性を確認
S166
新ルート鍵証明書を
記憶し、配布用ルート鍵
証明書、従前のルート鍵
証明書を廃棄
（従前のｸﾗｲｱﾝﾄ公開鍵
証明書も廃棄）
結果通知
S167
結果通知
S168

【図１３】


START
ルート鍵証明書
作成処理
（処理Ｓ）
サーバ装置の
ルート鍵証明書記憶処理
（処理１）
クライアント装置の
ルート鍵証明書記憶処理
（処理２）
サーバ装置の
公開鍵証明書記憶処理
（処理４）
クライアント装置の
公開鍵証明書記憶処理
（処理３）
サーバ装置のルート鍵
証明書書き換え処理
（処理５）
ｸﾗｲｱﾝﾄ装置のルート鍵
証明書書き換え処理
（処理６）
END

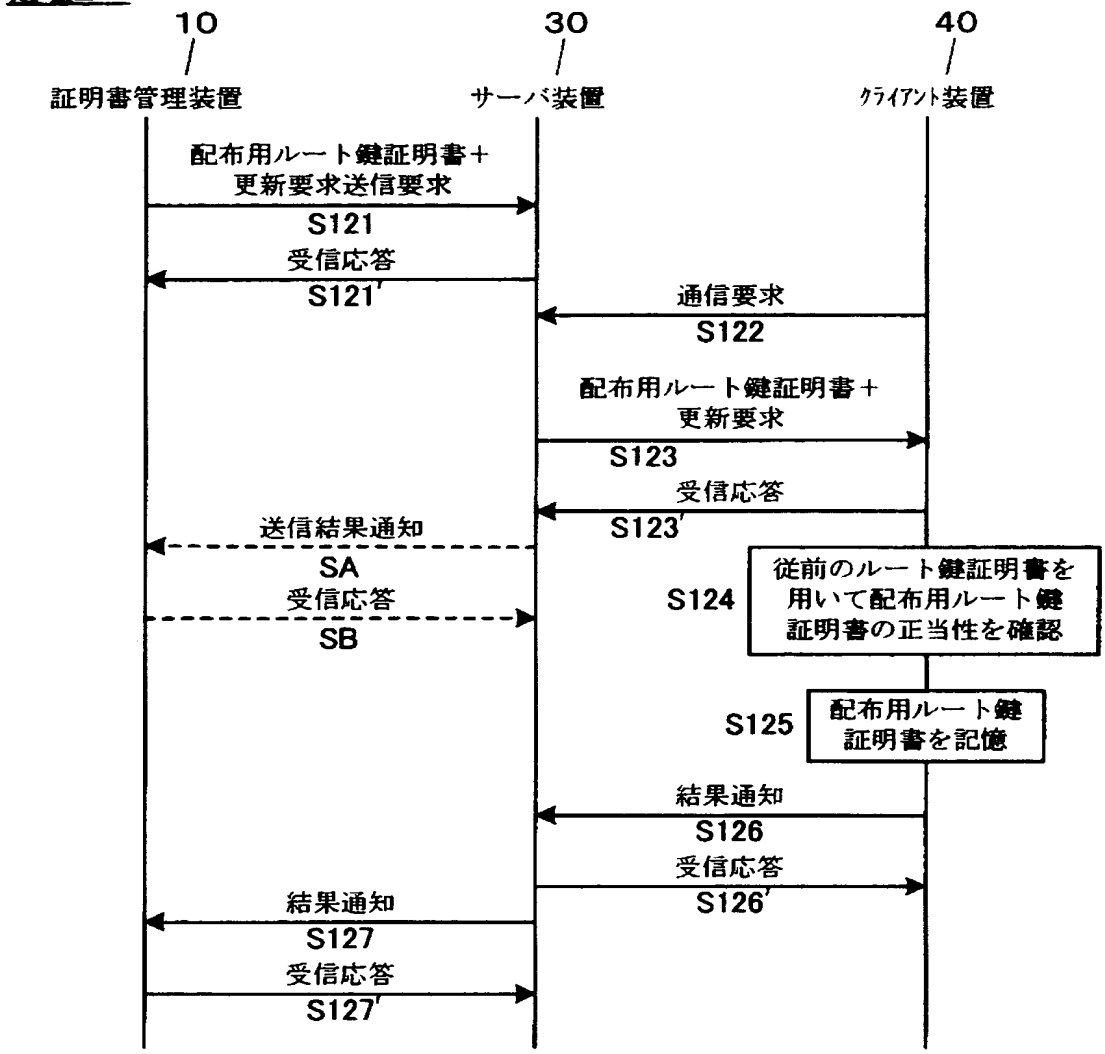
【図１４】

処理1′

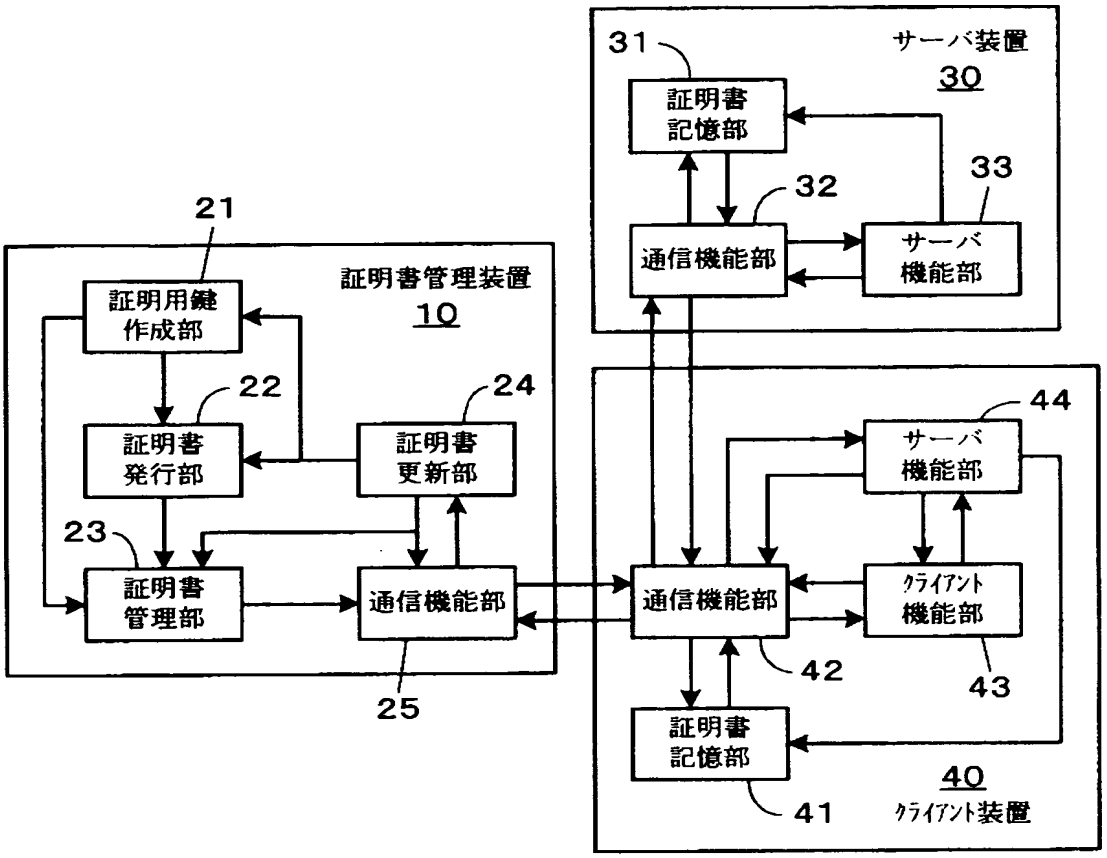

10
30
40
証明書管理装置
サーバ装置
ｸﾗｲｱﾝﾄ装置
配布用ルート鍵証明書＋
更新要求
S111
受信応答
S111′
S112
従前のルート鍵証明書を
用いて配布用ルート鍵
証明書の正当性を確認
S113
配布用ルート鍵
証明書を記憶
結果通知
S114
受信応答
S114′

【図１５】

処理2′

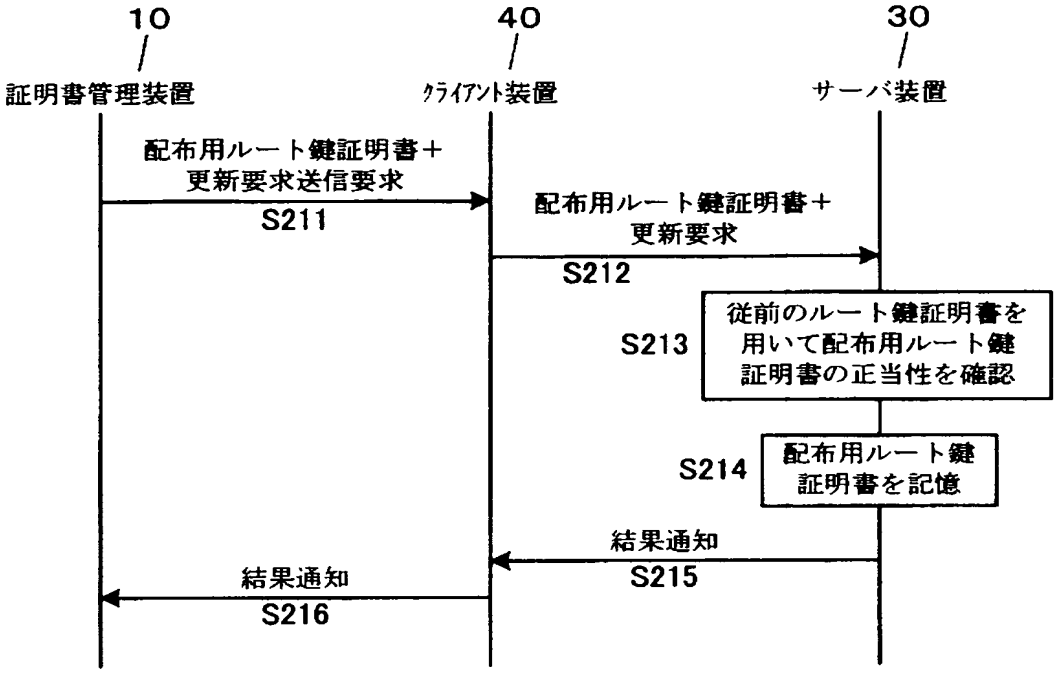

10
30
40
証明書管理装置
サーバ装置
ｸﾗｲｱﾝﾄ装置
配布用ルート鍵証明書＋
更新要求送信要求
S121
受信応答
S121′
通信要求
S122
配布用ルート鍵証明書＋
更新要求
S123
受信応答
S123′
送信結果通知
SA
受信応答
SB
S124
従前のルート鍵証明書を
用いて配布用ルート鍵
証明書の正当性を確認
S125
配布用ルート鍵
証明書を記憶
結果通知
S126
受信応答
S126′
結果通知
S127
受信応答
S127′

【図１６】


31
サーバ装置
30
証明書
記憶部
32
33
通信機能部
サーバ
機能部
21
証明書管理装置
10
証明用鍵
作成部
22
24
証明書
発行部
証明書
更新部
23
証明書
管理部
通信機能部
25
44
サーバ
機能部
通信機能部
ｸﾗｲｱﾝﾄ
機能部
42
43
証明書
記憶部
40
41
ｸﾗｲｱﾝﾄ装置

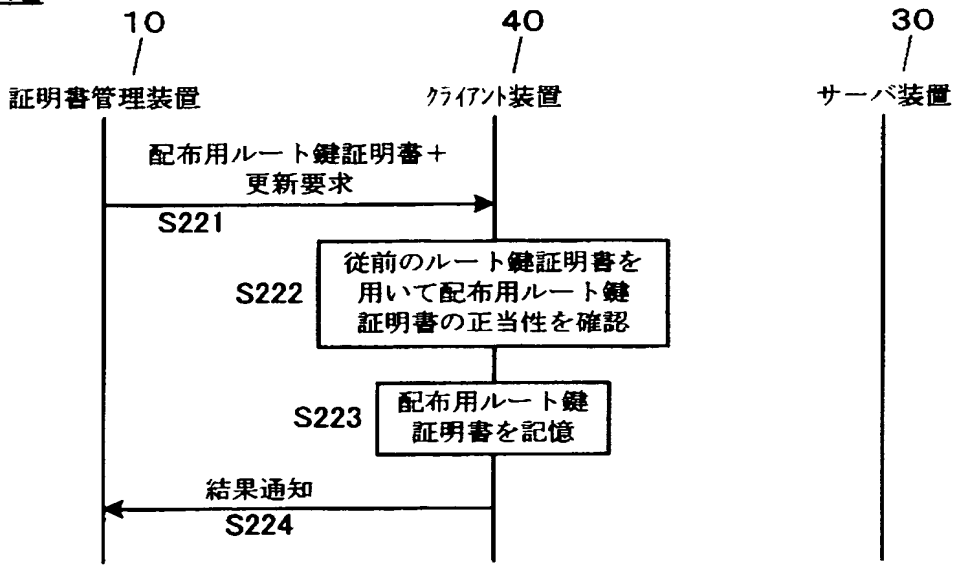
【図１７】

処理11

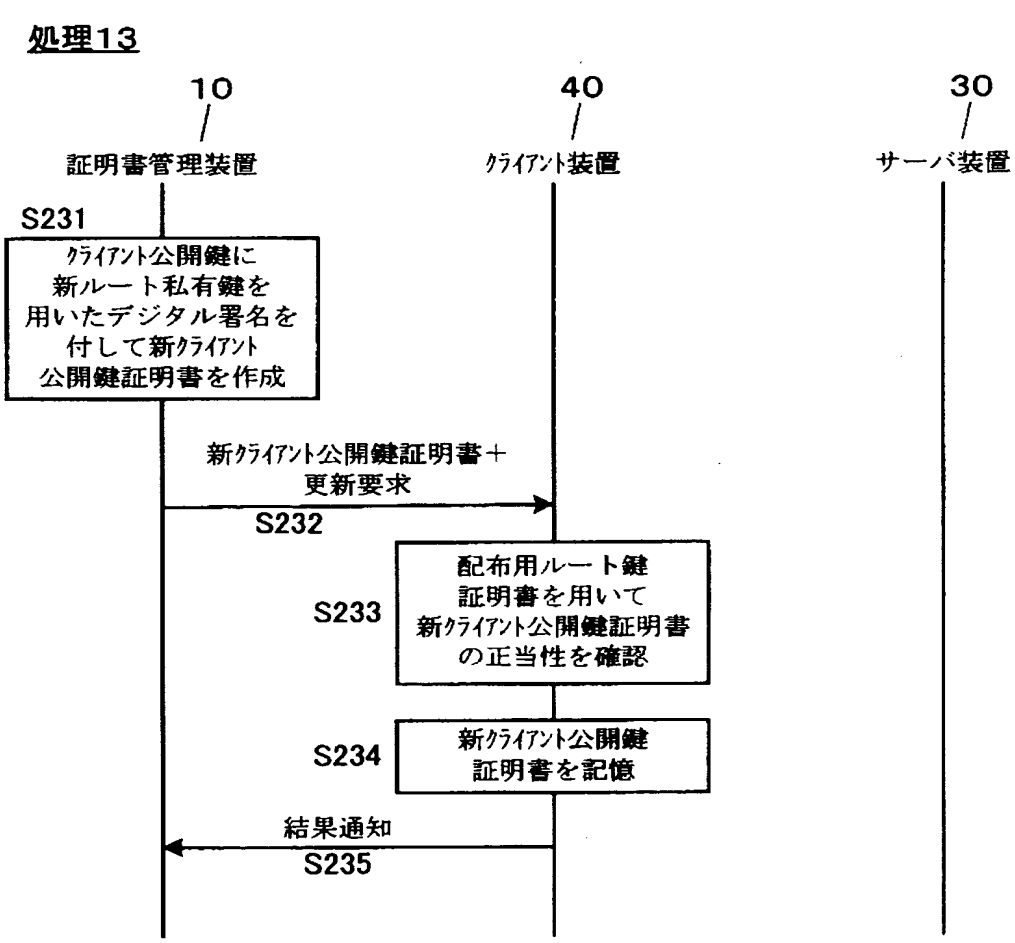



【図１８】

処理12

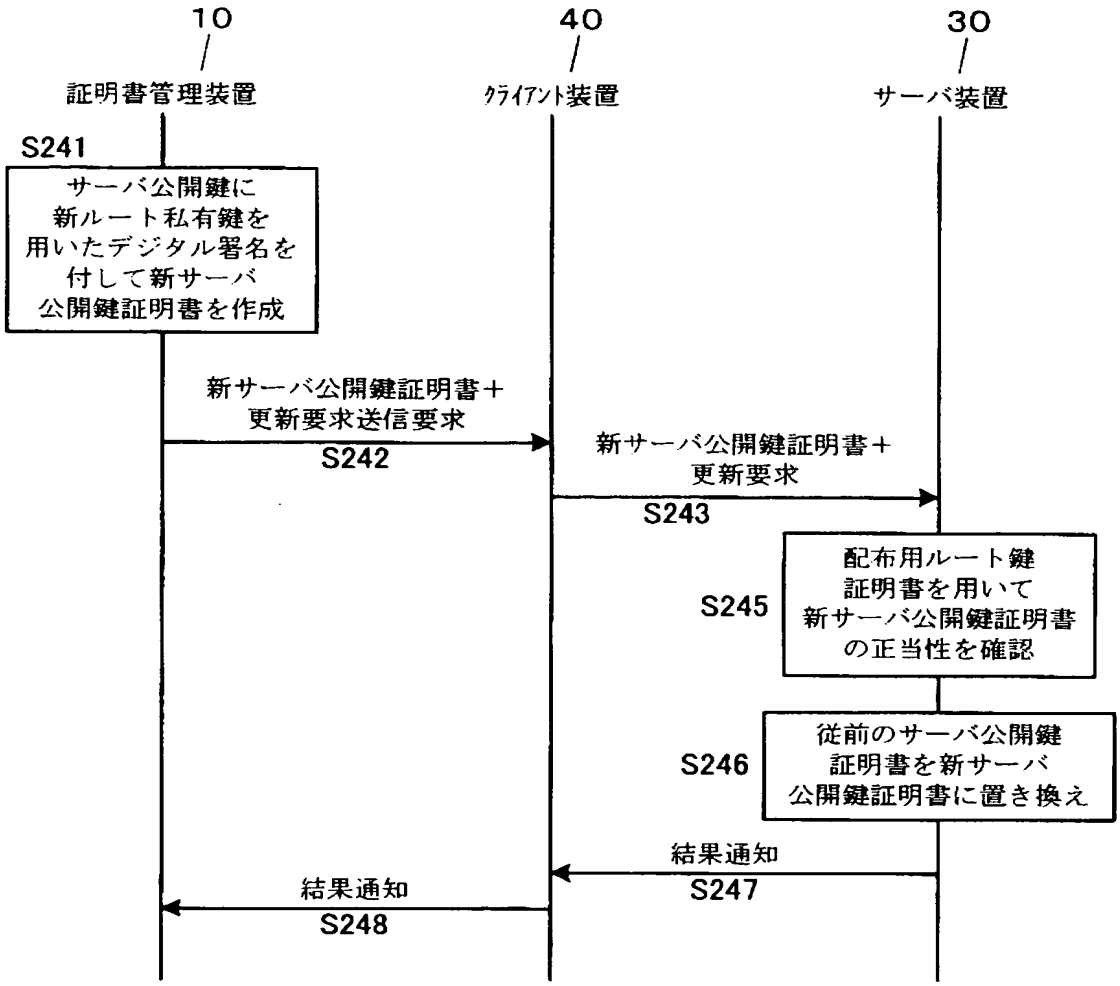


【図１９】


処理13
10
証明書管理装置
40
ｸﾗｲｱﾝﾄ装置
30
サーバ装置
S231
ｸﾗｲｱﾝﾄ公開鍵に
新ルート私有鍵を
用いたデジタル署名を
付して新ｸﾗｲｱﾝﾄ
公開鍵証明書を作成
新ｸﾗｲｱﾝﾄ公開鍵証明書＋
更新要求
S232
S233
配布用ルート鍵
証明書を用いて
新ｸﾗｲｱﾝﾄ公開鍵証明書
の正当性を確認
S234
新ｸﾗｲｱﾝﾄ公開鍵
証明書を記憶
結果通知
S235

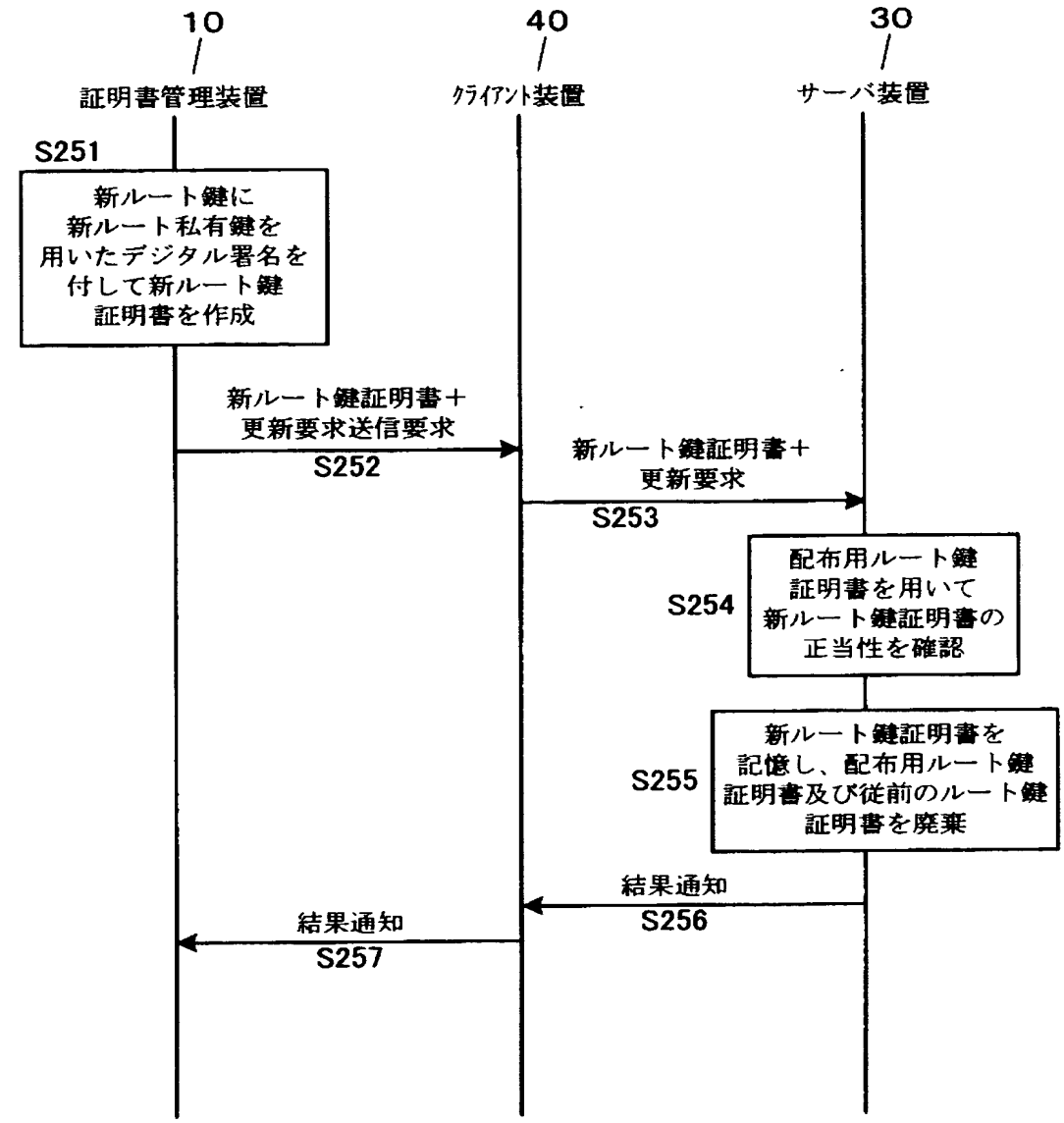
【図２０】

処理14


10
証明書管理装置
40
ｸﾗｲｱﾝﾄ装置
30
サーバ装置
S241
サーバ公開鍵に
新ルート私有鍵を
用いたデジタル署名を
付して新サーバ
公開鍵証明書を作成
新サーバ公開鍵証明書＋
更新要求送信要求
S242
新サーバ公開鍵証明書＋
更新要求
S243
S245
配布用ルート鍵
証明書を用いて
新サーバ公開鍵証明書
の正当性を確認
S246
従前のサーバ公開鍵
証明書を新サーバ
公開鍵証明書に置き換え
結果通知
S247
結果通知
S248

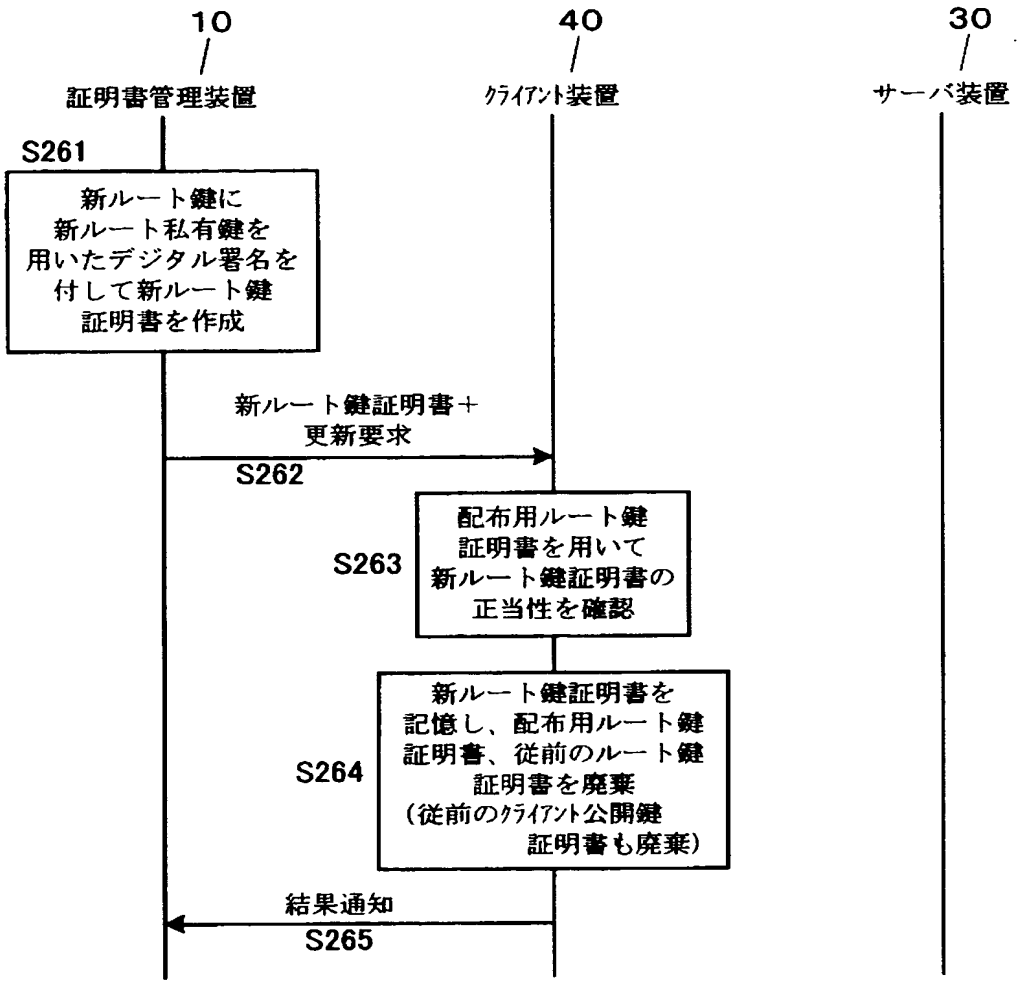
【図２１】

処理15

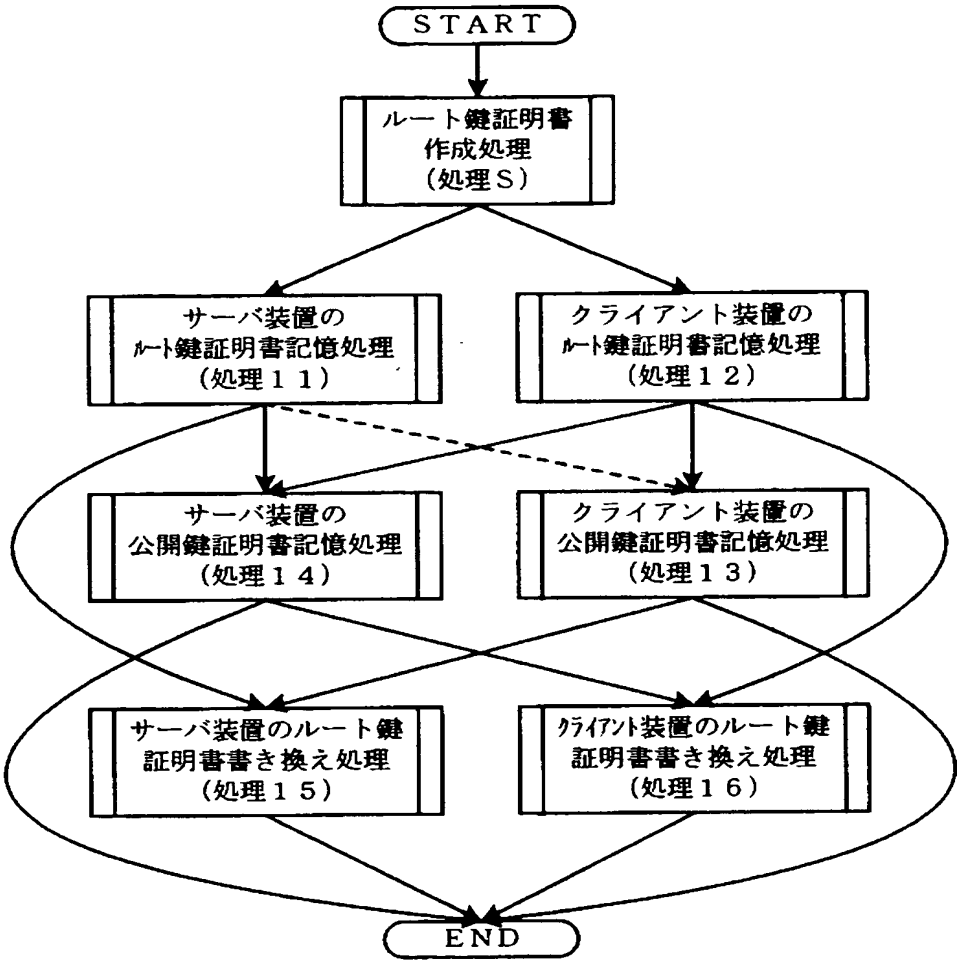

10
40
30
証明書管理装置
ｸﾗｲｱﾝﾄ装置
サーバ装置
S251
新ルート鍵に
新ルート私有鍵を
用いたデジタル署名を
付して新ルート鍵
証明書を作成
新ルート鍵証明書＋
更新要求送信要求
S252
新ルート鍵証明書＋
更新要求
S253
S254
配布用ルート鍵
証明書を用いて
新ルート鍵証明書の
正当性を確認
S255
新ルート鍵証明書を
記憶し、配布用ルート鍵
証明書及び従前のルート鍵
証明書を廃棄
結果通知
S256
結果通知
S257

【図２２】

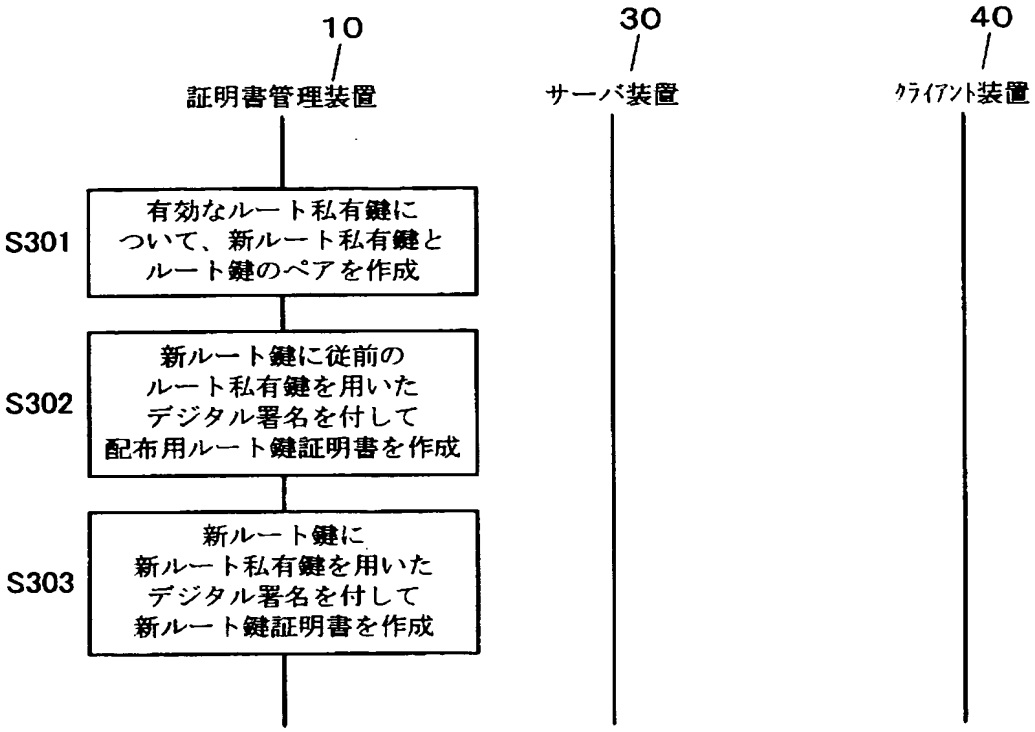
処理16


10
証明書管理装置
40
ｸﾗｲｱﾝﾄ装置
30
サーバ装置
S261
新ルート鍵に
新ルート私有鍵を
用いたデジタル署名を
付して新ルート鍵
証明書を作成
新ルート鍵証明書＋
更新要求
S262
S263
配布用ルート鍵
証明書を用いて
新ルート鍵証明書の
正当性を確認
S264
新ルート鍵証明書を
記憶し、配布用ルート鍵
証明書、従前のルート鍵
証明書を廃棄
（従前のｸﾗｲｱﾝﾄ公開鍵
証明書も廃棄）
結果通知
S265

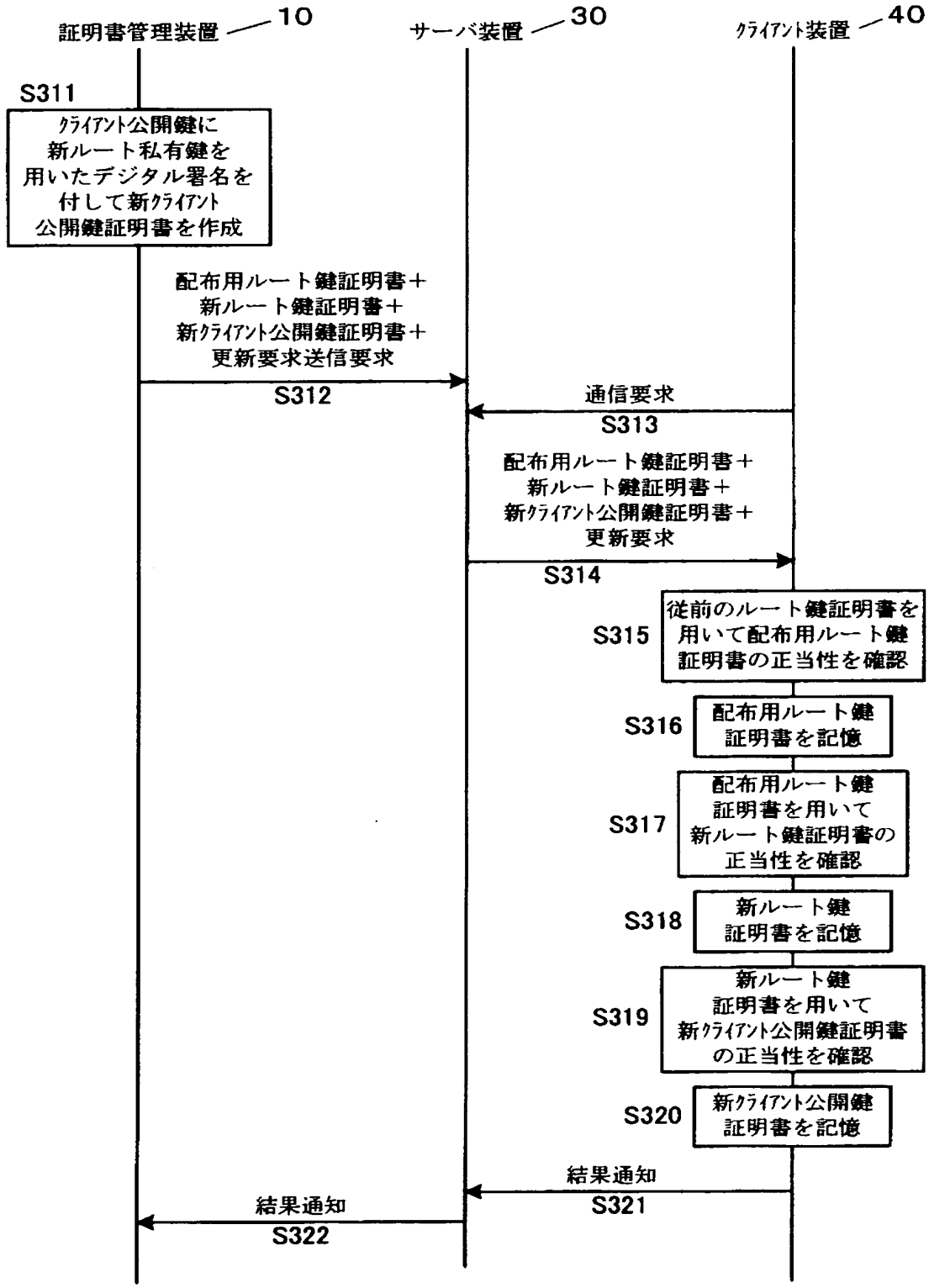
【図２３】


START
ルート鍵証明書
作成処理
（処理Ｓ）
サーバ装置の
ルート鍵証明書記憶処理
（処理１１）
クライアント装置の
ルート鍵証明書記憶処理
（処理１２）
サーバ装置の
公開鍵証明書記憶処理
（処理１４）
クライアント装置の
公開鍵証明書記憶処理
（処理１３）
サーバ装置のルート鍵
証明書書き換え処理
（処理１５）
クライアント装置のルート鍵
証明書書き換え処理
（処理１６）
END

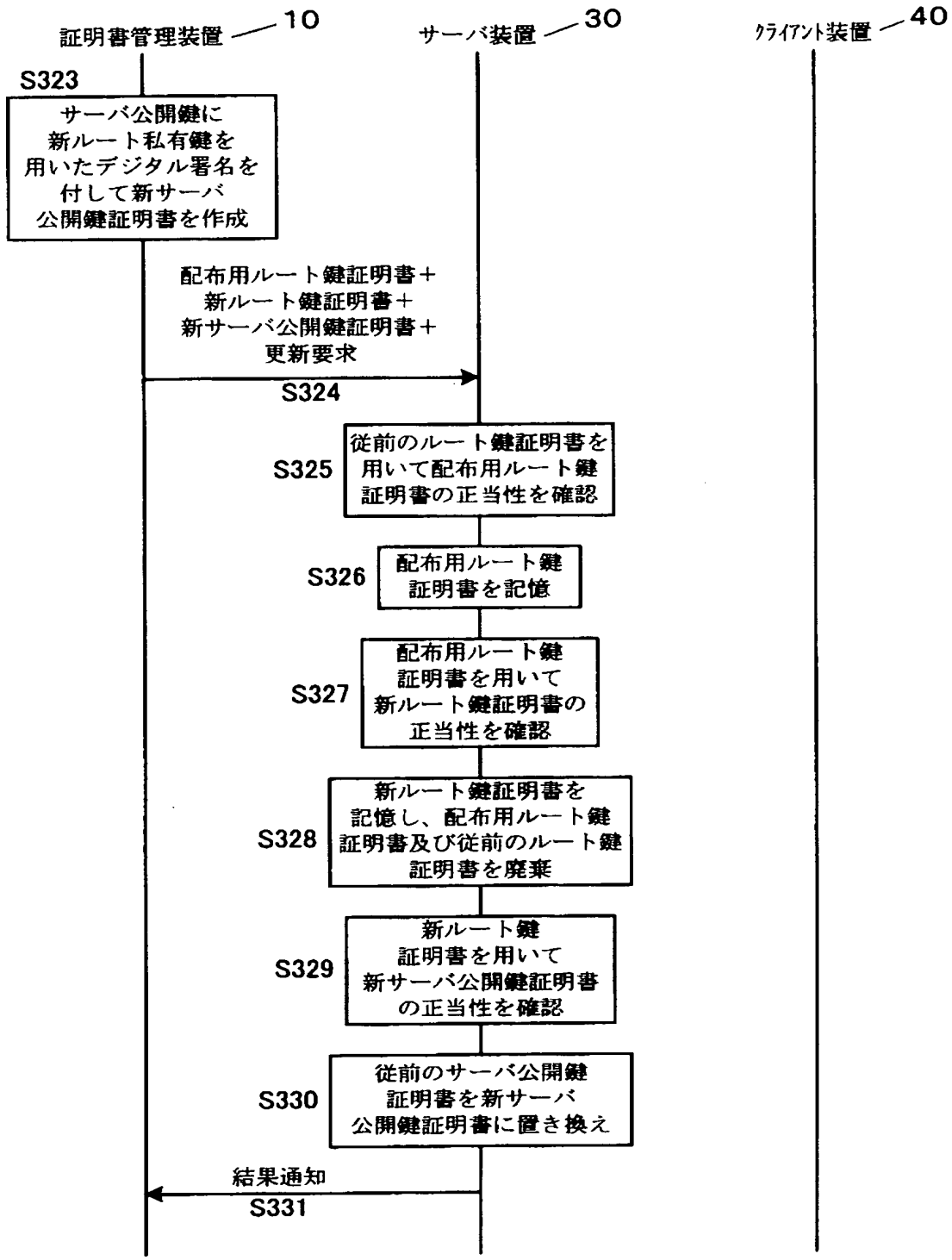
【図２４】


10
証明書管理装置
30
サーバ装置
40
ｸﾗｲｱﾝﾄ装置
S301
有効なルート私有鍵について、新ルート私有鍵とルート鍵のペアを作成
S302
新ルート鍵に従前のルート私有鍵を用いたデジタル署名を付して配布用ルート鍵証明書を作成
S303
新ルート鍵に新ルート私有鍵を用いたデジタル署名を付して新ルート鍵証明書を作成

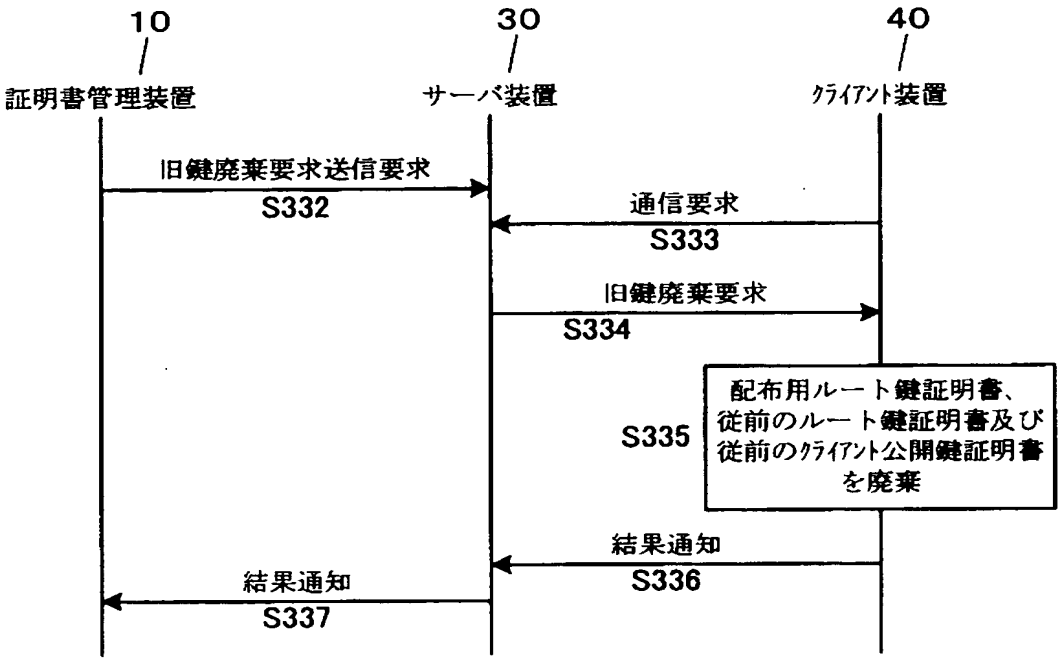
【図２５】


証明書管理装置
10
サーバ装置
30
ｸﾗｲｱﾝﾄ装置
40
S311
ｸﾗｲｱﾝﾄ公開鍵に
新ルート私有鍵を
用いたデジタル署名を
付して新ｸﾗｲｱﾝﾄ
公開鍵証明書を作成
配布用ルート鍵証明書＋
新ルート鍵証明書＋
新ｸﾗｲｱﾝﾄ公開鍵証明書＋
更新要求送信要求
S312
通信要求
S313
配布用ルート鍵証明書＋
新ルート鍵証明書＋
新ｸﾗｲｱﾝﾄ公開鍵証明書＋
更新要求
S314
S315
従前のルート鍵証明書を
用いて配布用ルート鍵
証明書の正当性を確認
S316
配布用ルート鍵
証明書を記憶
S317
配布用ルート鍵
証明書を用いて
新ルート鍵証明書の
正当性を確認
S318
新ルート鍵
証明書を記憶
S319
新ルート鍵
証明書を用いて
新ｸﾗｲｱﾝﾄ公開鍵証明書
の正当性を確認
S320
新ｸﾗｲｱﾝﾄ公開鍵
証明書を記憶
結果通知
S321
結果通知
S322

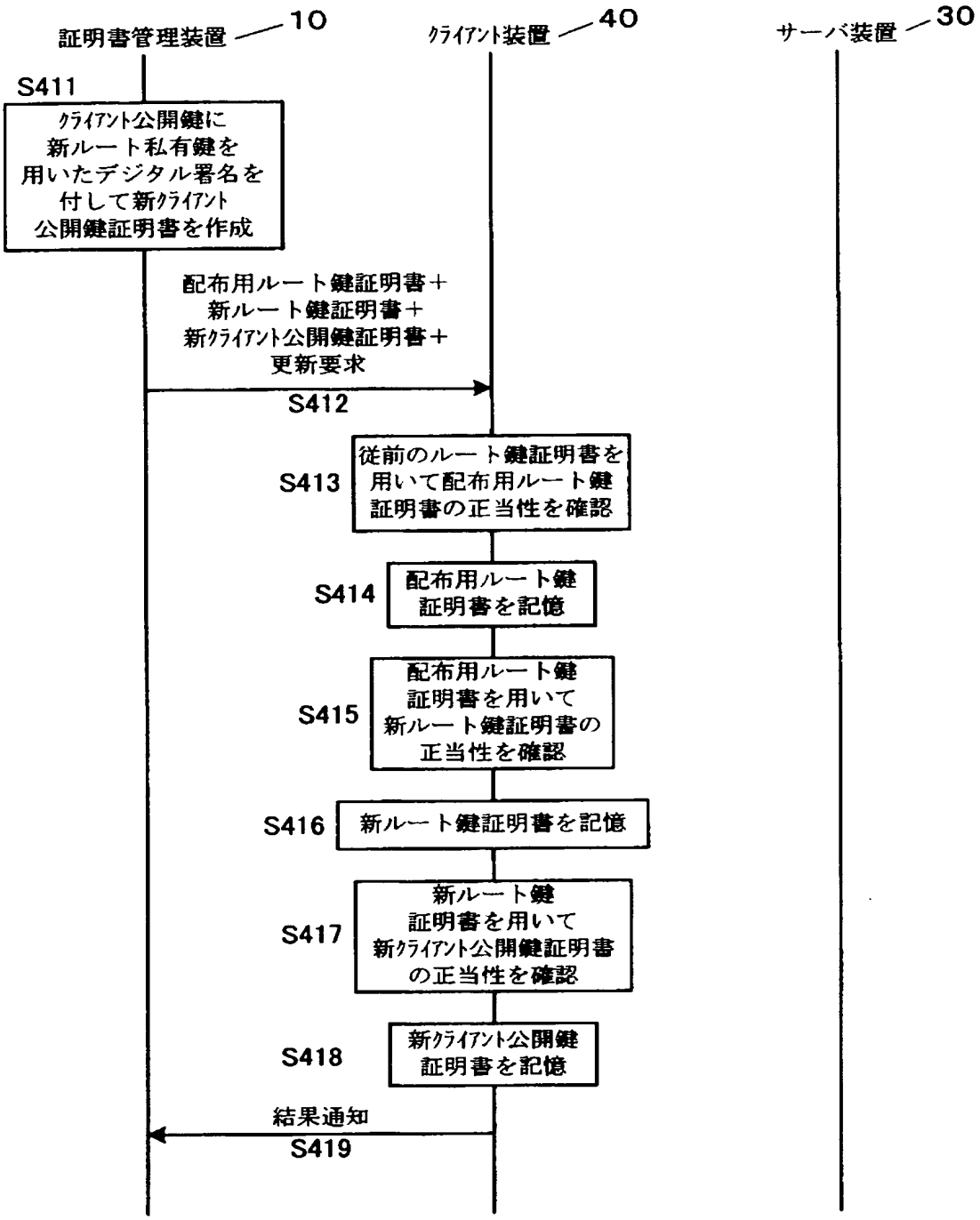
【図２６】


証明書管理装置
10
サーバ装置
30
ｸﾗｲｱﾝﾄ装置
40
S323
サーバ公開鍵に新ルート私有鍵を用いたデジタル署名を付して新サーバ公開鍵証明書を作成
配布用ルート鍵証明書＋新ルート鍵証明書＋新サーバ公開鍵証明書＋更新要求
S324
S325
従前のルート鍵証明書を用いて配布用ルート鍵証明書の正当性を確認
S326
配布用ルート鍵証明書を記憶
S327
配布用ルート鍵証明書を用いて新ルート鍵証明書の正当性を確認
S328
新ルート鍵証明書を記憶し、配布用ルート鍵証明書及び従前のルート鍵証明書を廃棄
S329
新ルート鍵証明書を用いて新サーバ公開鍵証明書の正当性を確認
S330
従前のサーバ公開鍵証明書を新サーバ公開鍵証明書に置き換え
結果通知
S331

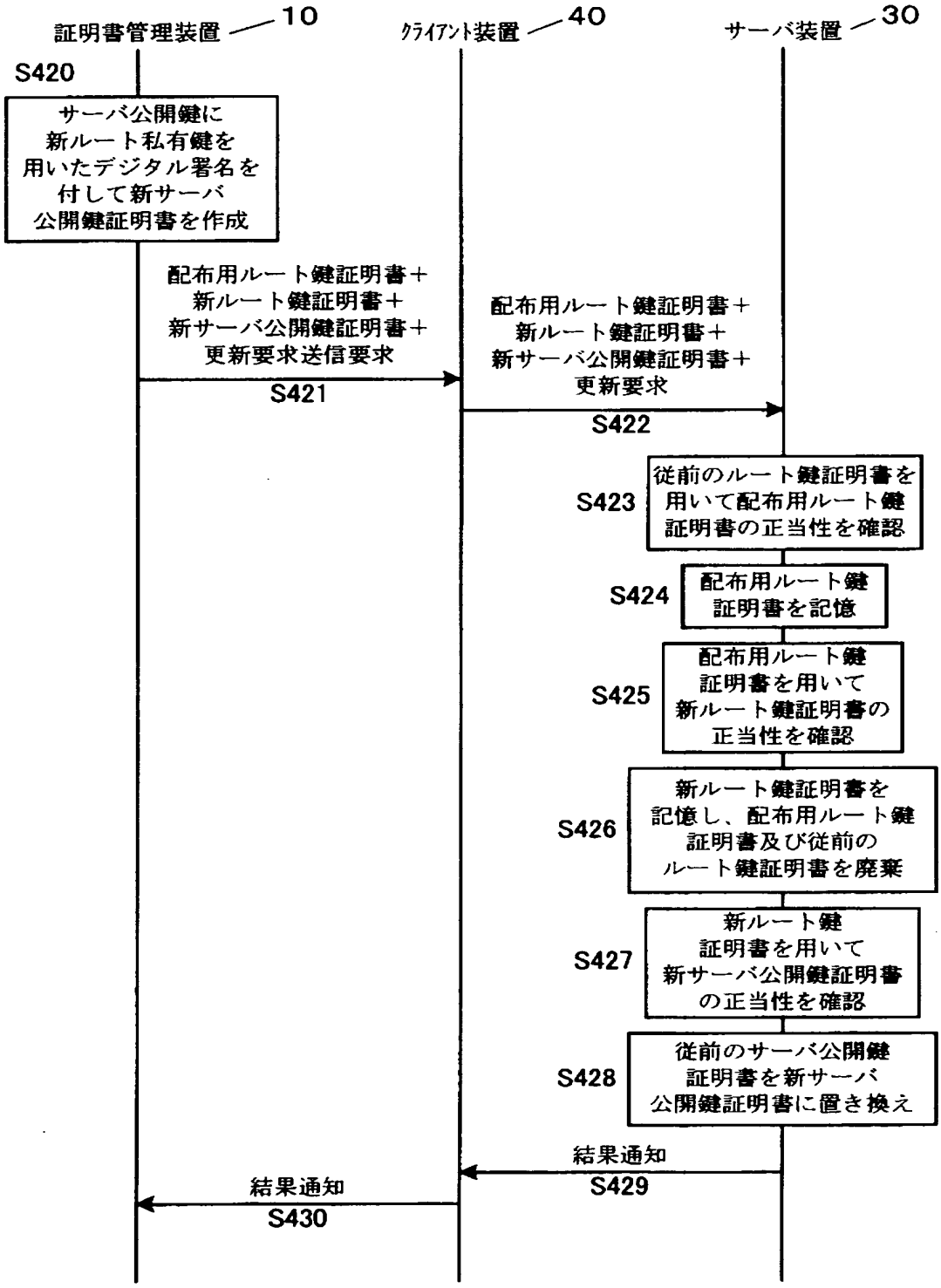
【図２７】


10
30
40
証明書管理装置
サーバ装置
ｸﾗｲｱﾝﾄ装置
旧鍵廃棄要求送信要求
S332
通信要求
S333
旧鍵廃棄要求
S334
S335
配布用ルート鍵証明書、
従前のルート鍵証明書及び
従前のｸﾗｲｱﾝﾄ公開鍵証明書
を廃棄
結果通知
S336
結果通知
S337

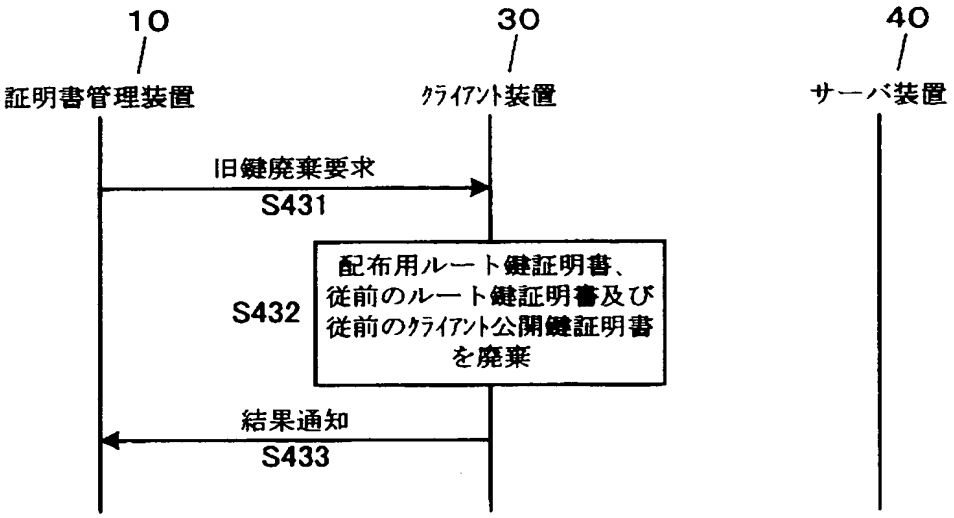
【図２８】


証明書管理装置
10
クライアント装置
40
サーバ装置
30
S411
クライアント公開鍵に新ルート私有鍵を用いたデジタル署名を付して新クライアント公開鍵証明書を作成
配布用ルート鍵証明書＋新ルート鍵証明書＋新クライアント公開鍵証明書＋更新要求
S412
S413
従前のルート鍵証明書を用いて配布用ルート鍵証明書の正当性を確認
S414
配布用ルート鍵証明書を記憶
S415
配布用ルート鍵証明書を用いて新ルート鍵証明書の正当性を確認
S416
新ルート鍵証明書を記憶
S417
新ルート鍵証明書を用いて新クライアント公開鍵証明書の正当性を確認
S418
新クライアント公開鍵証明書を記憶
結果通知
S419

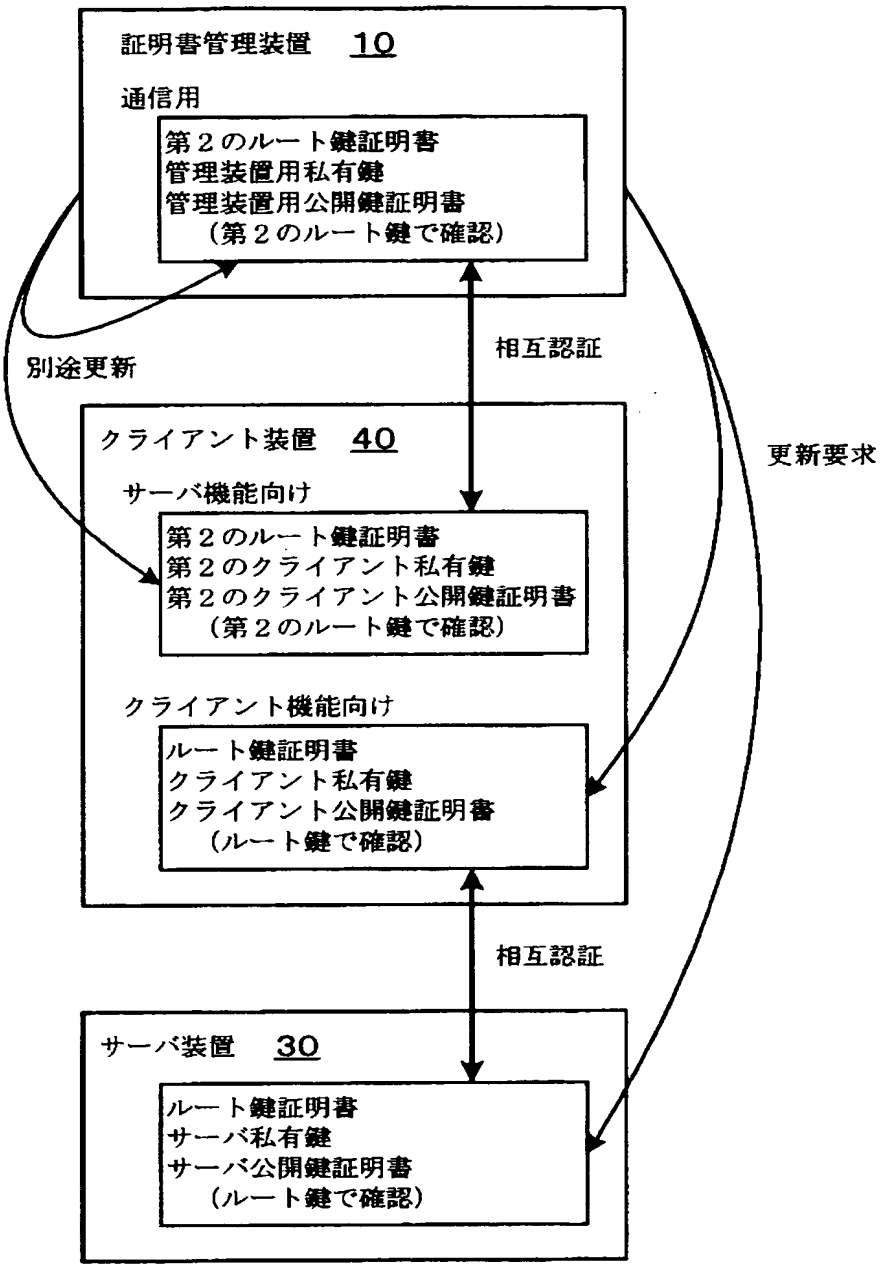
【図２９】


証明書管理装置
10
ｸﾗｲｱﾝﾄ装置
40
サーバ装置
30
S420
サーバ公開鍵に新ルート私有鍵を用いたデジタル署名を付して新サーバ公開鍵証明書を作成
配布用ルート鍵証明書＋新ルート鍵証明書＋新サーバ公開鍵証明書＋更新要求送信要求
S421
配布用ルート鍵証明書＋新ルート鍵証明書＋新サーバ公開鍵証明書＋更新要求
S422
S423
従前のルート鍵証明書を用いて配布用ルート鍵証明書の正当性を確認
S424
配布用ルート鍵証明書を記憶
S425
配布用ルート鍵証明書を用いて新ルート鍵証明書の正当性を確認
S426
新ルート鍵証明書を記憶し、配布用ルート鍵証明書及び従前のルート鍵証明書を廃棄
S427
新ルート鍵証明書を用いて新サーバ公開鍵証明書の正当性を確認
S428
従前のサーバ公開鍵証明書を新サーバ公開鍵証明書に置き換え
結果通知
S429
結果通知
S430

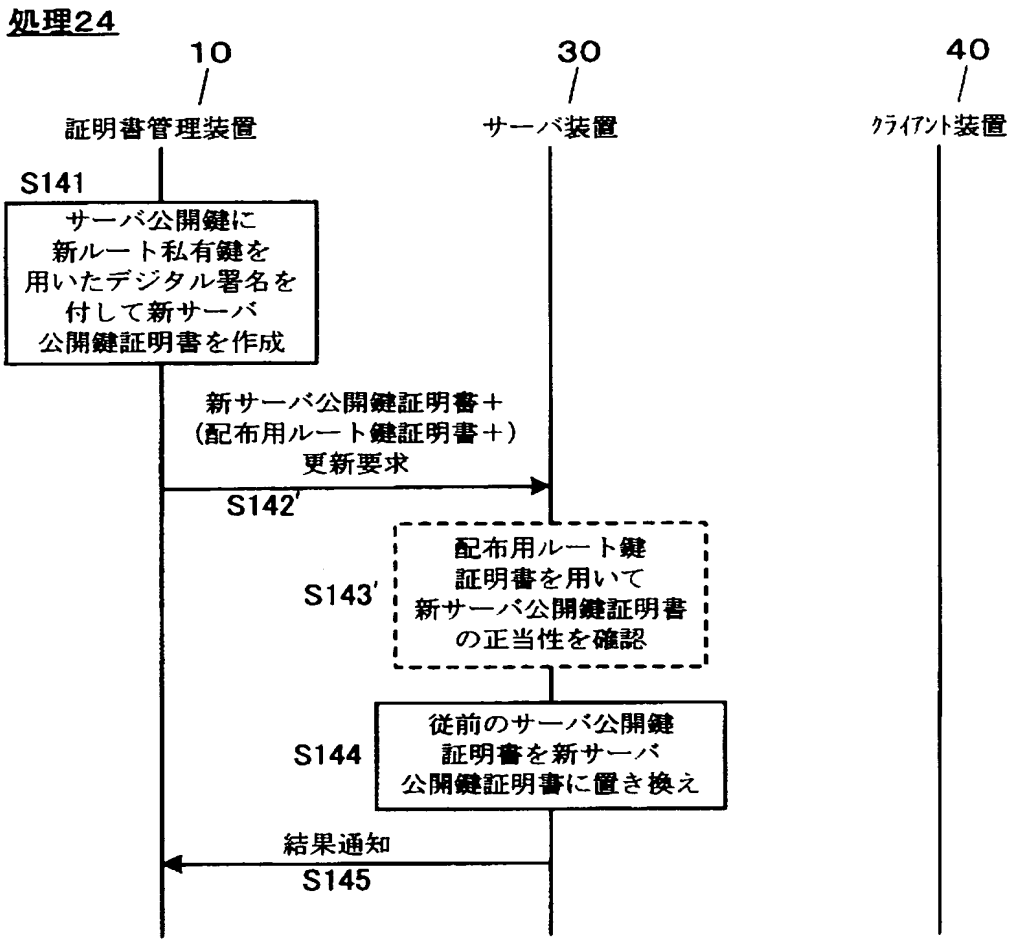
【図３０】


10
30
40
証明書管理装置
ｸﾗｲｱﾝﾄ装置
サーバ装置
旧鍵廃棄要求
S431
S432
配布用ルート鍵証明書、
従前のルート鍵証明書及び
従前のｸﾗｲｱﾝﾄ公開鍵証明書
を廃棄
結果通知
S433

【図３１】

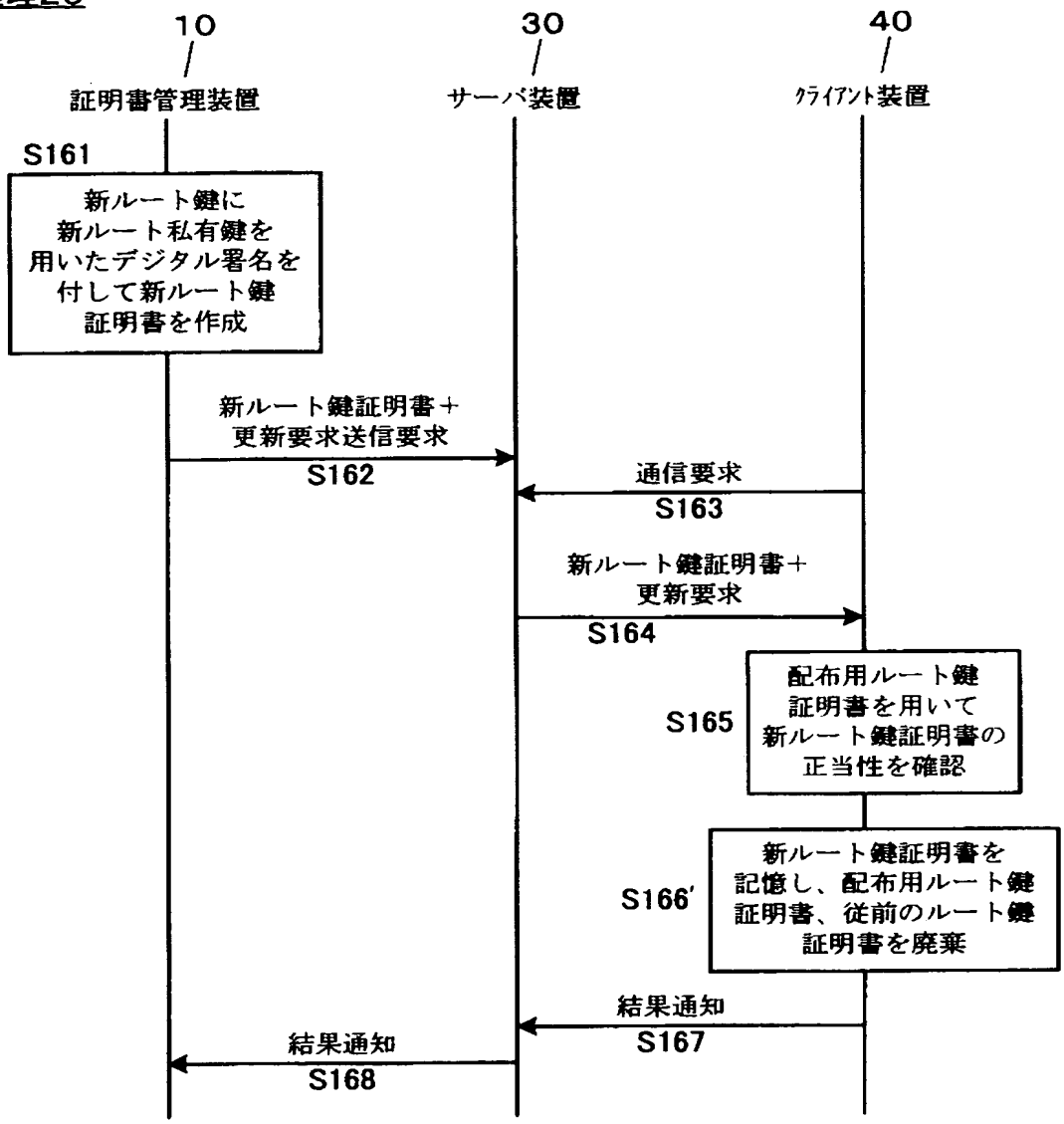

証明書管理装置　10
通信用
第２のルート鍵証明書
管理装置用私有鍵
管理装置用公開鍵証明書
（第２のルート鍵で確認）
別途更新
相互認証
クライアント装置　40
更新要求
サーバ機能向け
第２のルート鍵証明書
第２のクライアント私有鍵
第２のクライアント公開鍵証明書
（第２のルート鍵で確認）
クライアント機能向け
ルート鍵証明書
クライアント私有鍵
クライアント公開鍵証明書
（ルート鍵で確認）
相互認証
サーバ装置　30
ルート鍵証明書
サーバ私有鍵
サーバ公開鍵証明書
（ルート鍵で確認）

【図３２】

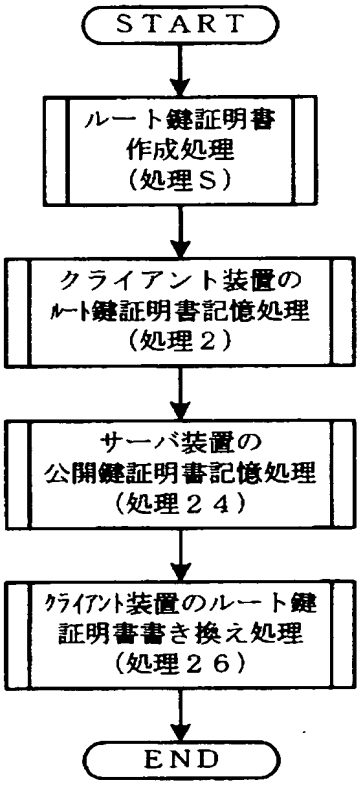

処理24
10
30
40
証明書管理装置
サーバ装置
ｸﾗｲｱﾝﾄ装置
S141
サーバ公開鍵に
新ルート私有鍵を
用いたデジタル署名を
付して新サーバ
公開鍵証明書を作成
新サーバ公開鍵証明書＋
(配布用ルート鍵証明書＋)
更新要求
S142'
S143'
配布用ルート鍵
証明書を用いて
新サーバ公開鍵証明書
の正当性を確認
S144
従前のサーバ公開鍵
証明書を新サーバ
公開鍵証明書に置き換え
結果通知
S145

【図３３】

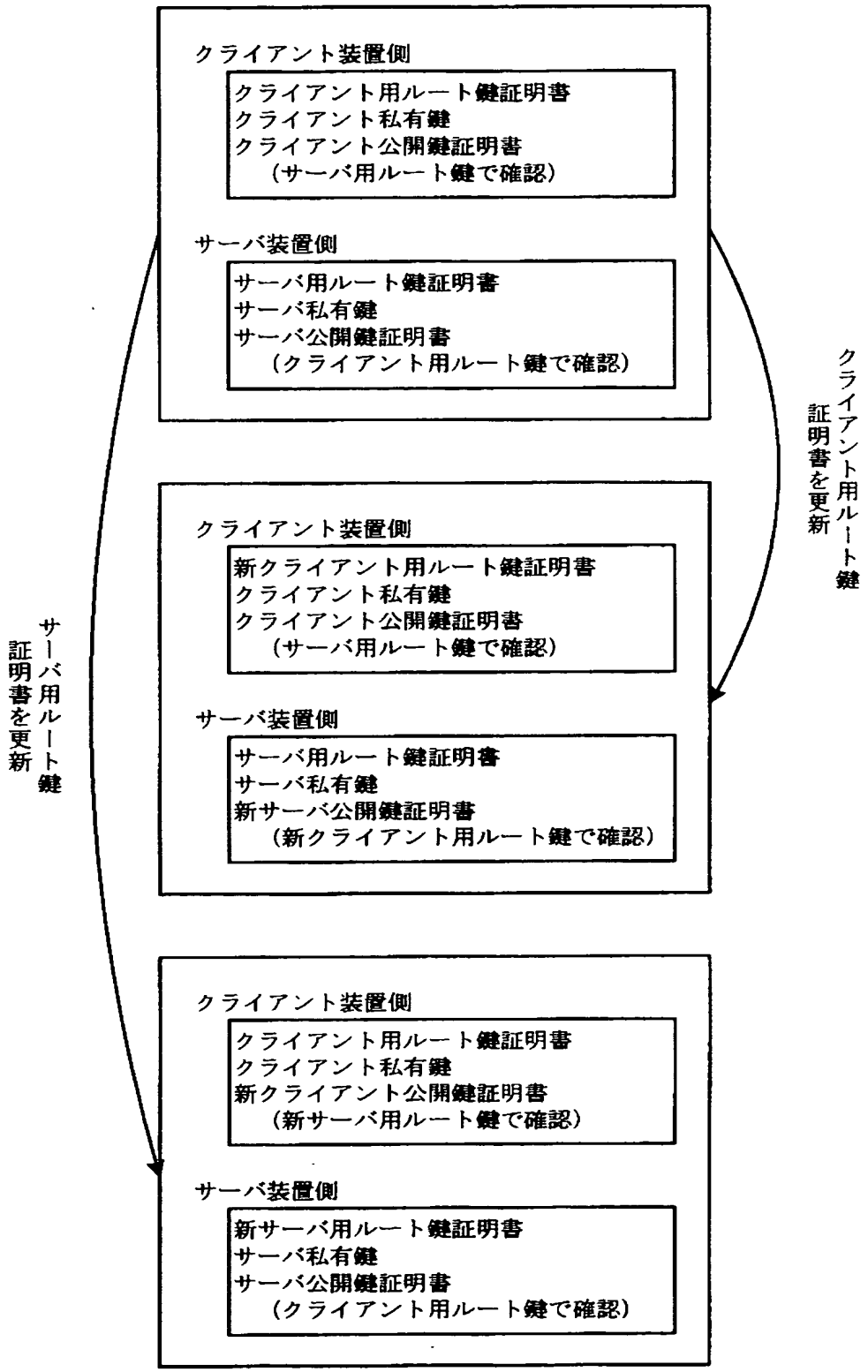
処理26


10
30
40
証明書管理装置
サーバ装置
ｸﾗｲｱﾝﾄ装置
S161
新ルート鍵に
新ルート私有鍵を
用いたデジタル署名を
付して新ルート鍵
証明書を作成
新ルート鍵証明書＋
更新要求送信要求
S162
通信要求
S163
新ルート鍵証明書＋
更新要求
S164
S165
配布用ルート鍵
証明書を用いて
新ルート鍵証明書の
正当性を確認
S166'
新ルート鍵証明書を
記憶し、配布用ルート鍵
証明書、従前のルート鍵
証明書を廃棄
結果通知
S167
結果通知
S168

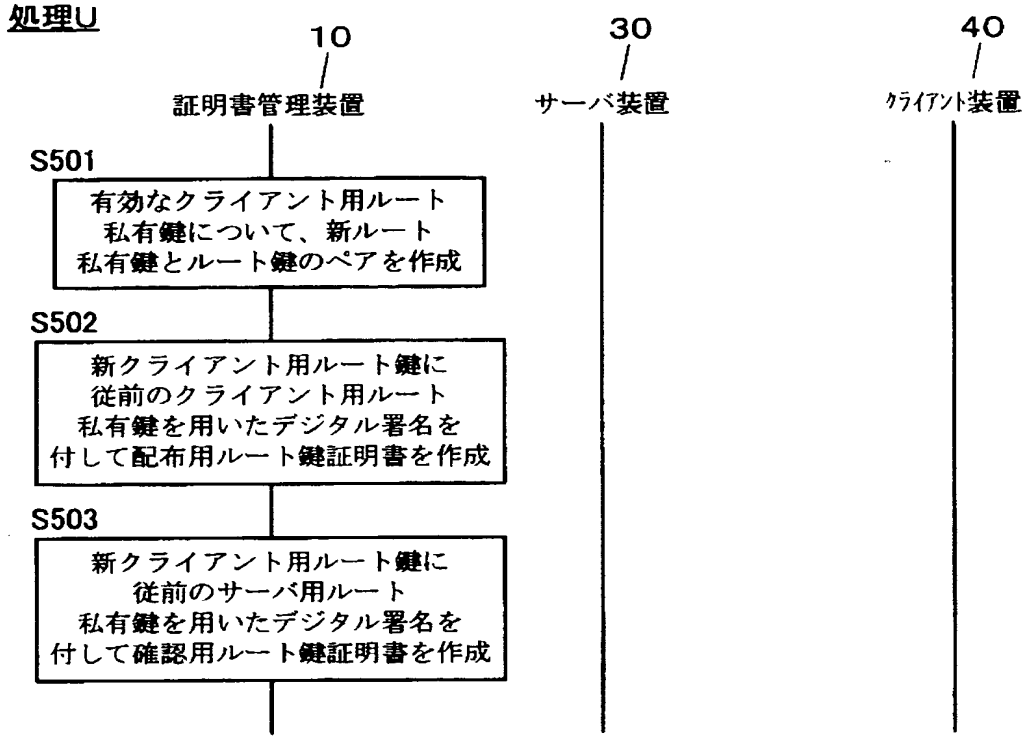
【図３４】


START
ルート鍵証明書
作成処理
（処理Ｓ）
クライアント装置の
ルート鍵証明書記憶処理
（処理２）
サーバ装置の
公開鍵証明書記憶処理
（処理２４）
ｸﾗｲｱﾝﾄ装置のルート鍵
証明書書き換え処理
（処理２６）
END

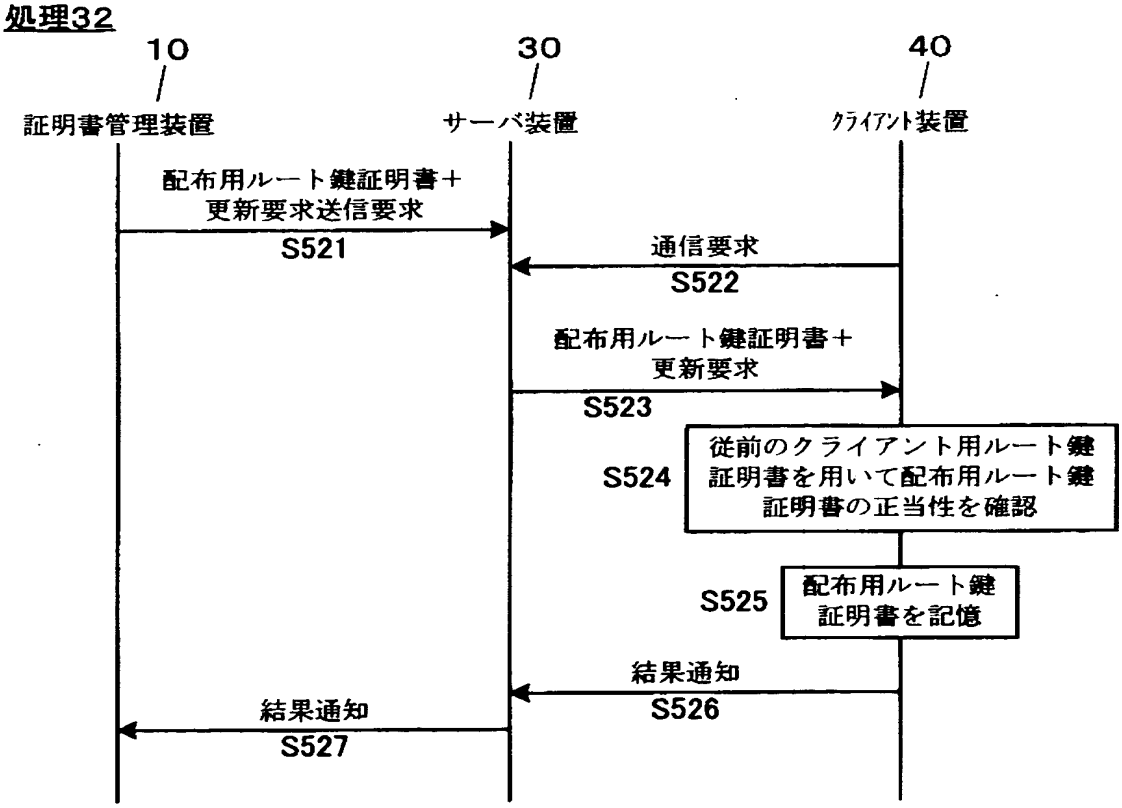
【図３５】


クライアント装置側
クライアント用ルート鍵証明書
クライアント私有鍵
クライアント公開鍵証明書
（サーバ用ルート鍵で確認）
サーバ装置側
サーバ用ルート鍵証明書
サーバ私有鍵
サーバ公開鍵証明書
（クライアント用ルート鍵で確認）
クライアント用ルート鍵証明書を更新
クライアント装置側
新クライアント用ルート鍵証明書
クライアント私有鍵
クライアント公開鍵証明書
（サーバ用ルート鍵で確認）
サーバ装置側
サーバ用ルート鍵証明書
サーバ私有鍵
新サーバ公開鍵証明書
（新クライアント用ルート鍵で確認）
サーバ用ルート鍵証明書を更新
クライアント装置側
クライアント用ルート鍵証明書
クライアント私有鍵
新クライアント公開鍵証明書
（新サーバ用ルート鍵で確認）
サーバ装置側
新サーバ用ルート鍵証明書
サーバ私有鍵
サーバ公開鍵証明書
（クライアント用ルート鍵で確認）

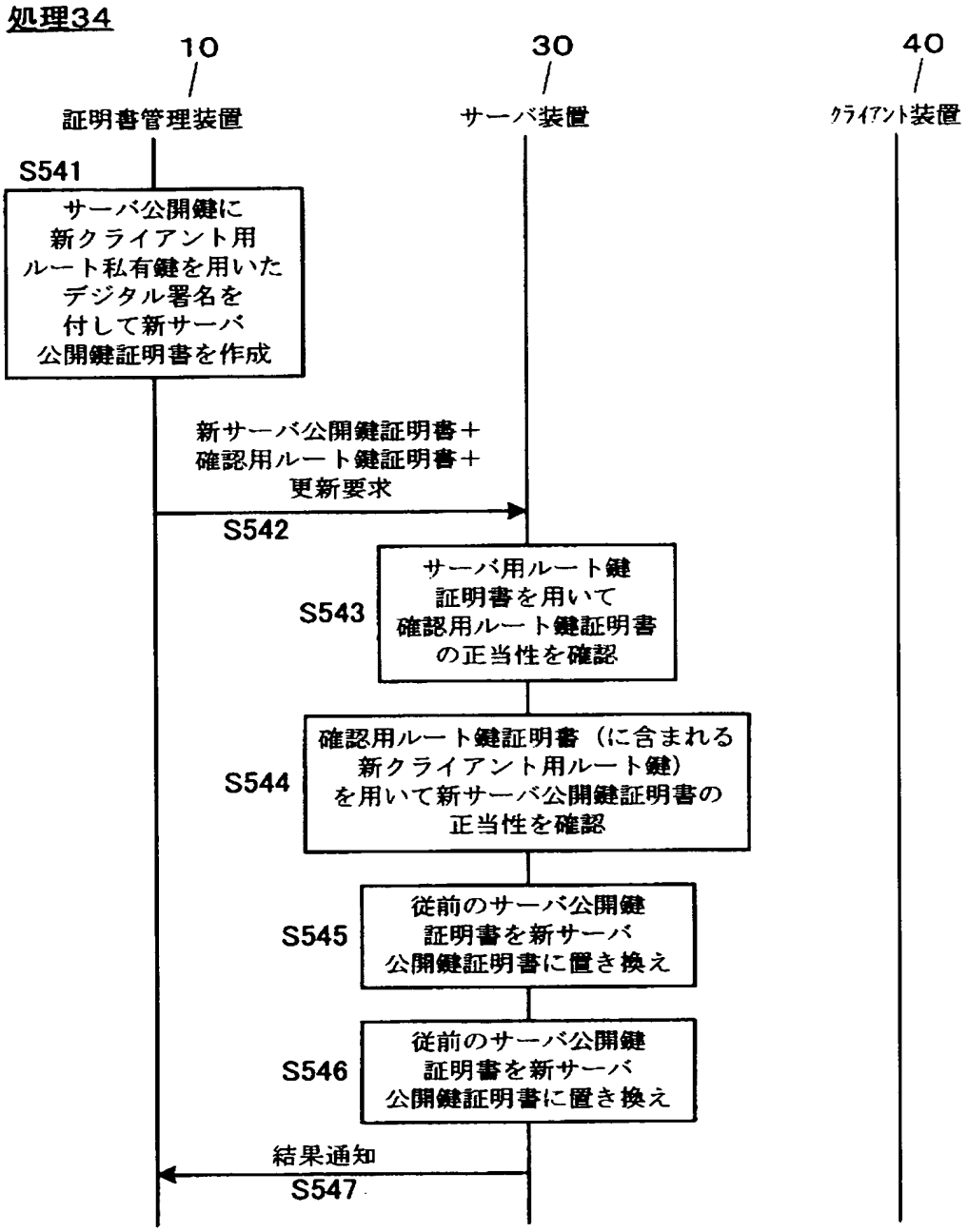
【図３６】


処理U
10
証明書管理装置
30
サーバ装置
40
ｸﾗｲｱﾝﾄ装置
S501
有効なクライアント用ルート
私有鍵について、新ルート
私有鍵とルート鍵のペアを作成
S502
新クライアント用ルート鍵に
従前のクライアント用ルート
私有鍵を用いたデジタル署名を
付して配布用ルート鍵証明書を作成
S503
新クライアント用ルート鍵に
従前のサーバ用ルート
私有鍵を用いたデジタル署名を
付して確認用ルート鍵証明書を作成

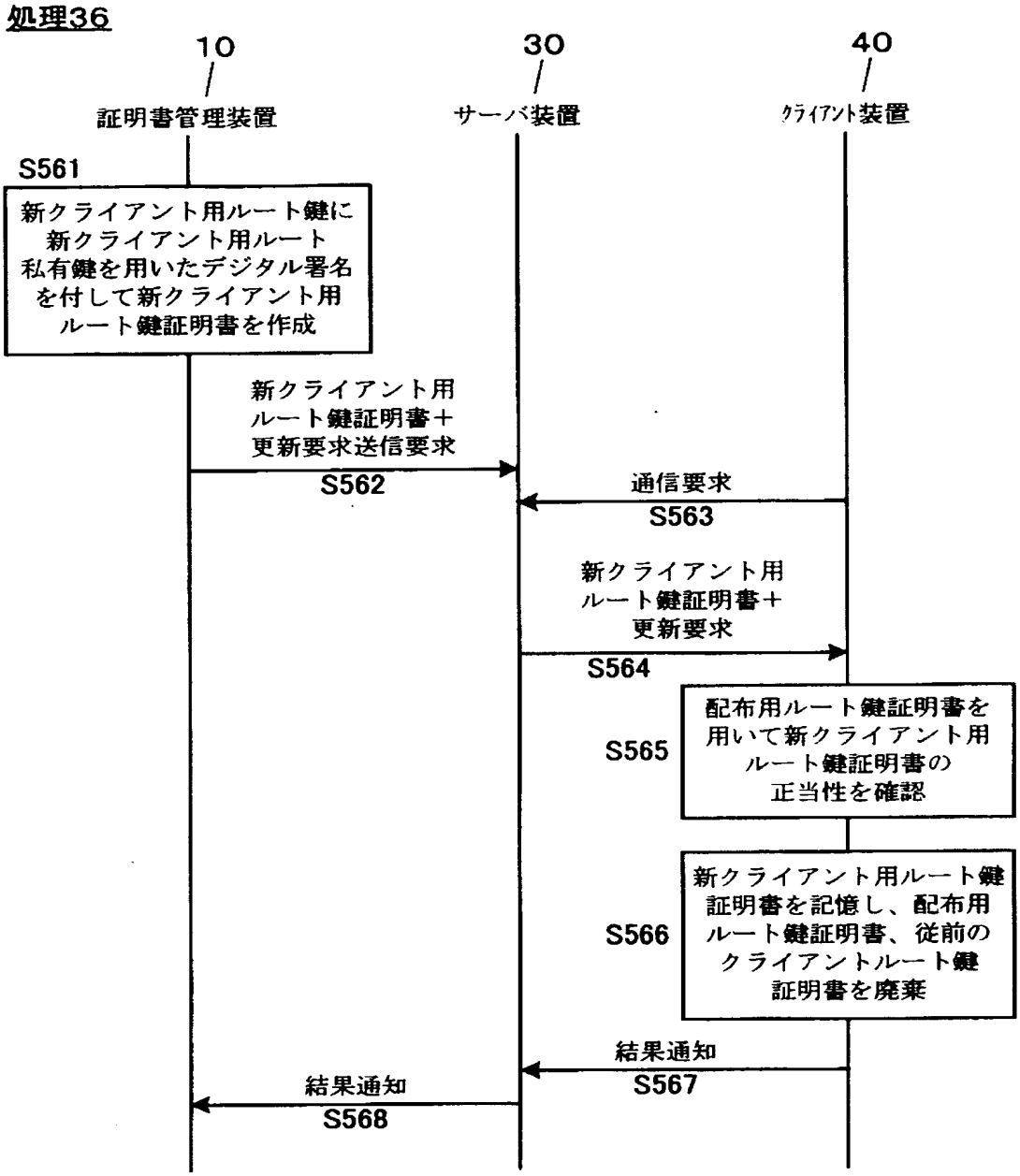
【図３７】


処理32
10
証明書管理装置
30
サーバ装置
40
ｸﾗｲｱﾝﾄ装置
配布用ルート鍵証明書＋
更新要求送信要求
S521
通信要求
S522
配布用ルート鍵証明書＋
更新要求
S523
S524
従前のクライアント用ルート鍵
証明書を用いて配布用ルート鍵
証明書の正当性を確認
S525
配布用ルート鍵
証明書を記憶
結果通知
S526
結果通知
S527

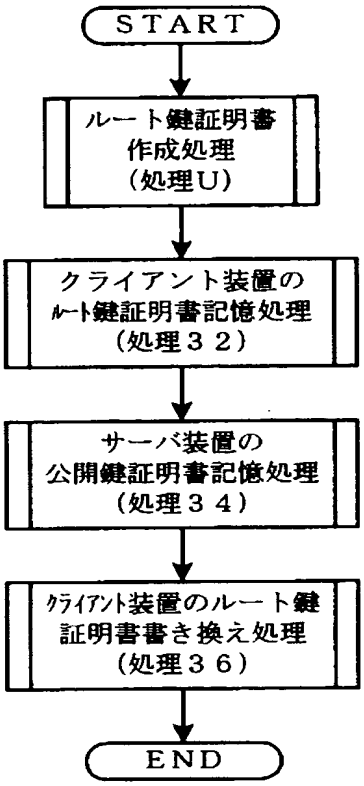
【図３８】


処理34
10
30
40
証明書管理装置
サーバ装置
ｸﾗｲｱﾝﾄ装置
S541
サーバ公開鍵に
新クライアント用
ルート私有鍵を用いた
デジタル署名を
付して新サーバ
公開鍵証明書を作成
新サーバ公開鍵証明書＋
確認用ルート鍵証明書＋
更新要求
S542
S543
サーバ用ルート鍵
証明書を用いて
確認用ルート鍵証明書
の正当性を確認
S544
確認用ルート鍵証明書（に含まれる
新クライアント用ルート鍵）
を用いて新サーバ公開鍵証明書の
正当性を確認
S545
従前のサーバ公開鍵
証明書を新サーバ
公開鍵証明書に置き換え
S546
従前のサーバ公開鍵
証明書を新サーバ
公開鍵証明書に置き換え
結果通知
S547

【図３９】

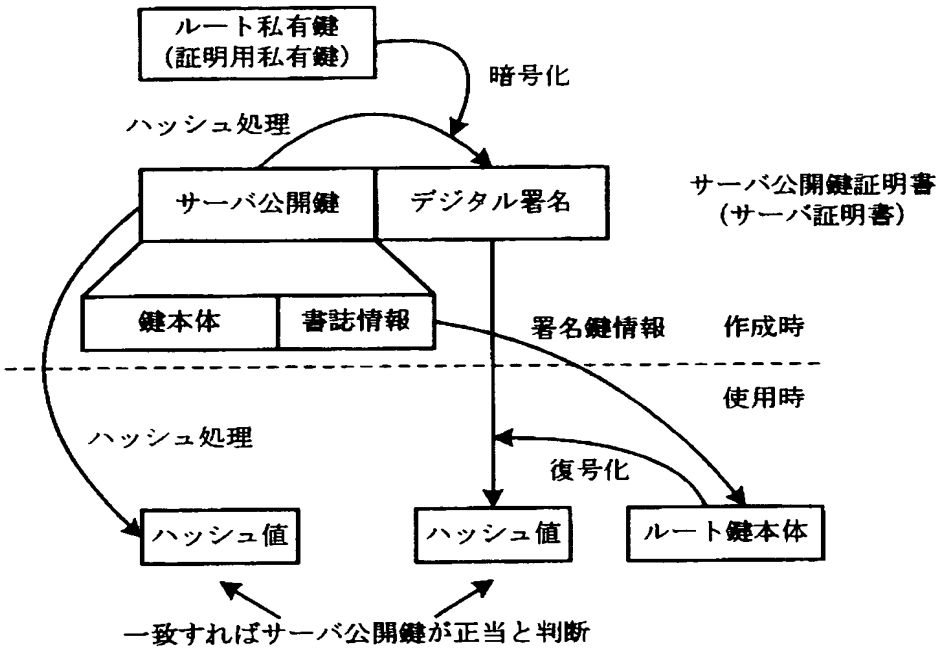

処理36
10
証明書管理装置
30
サーバ装置
40
ｸﾗｲｱﾝﾄ装置
S561
新クライアント用ルート鍵に新クライアント用ルート私有鍵を用いたデジタル署名を付して新クライアント用ルート鍵証明書を作成
新クライアント用ルート鍵証明書＋更新要求送信要求
S562
通信要求
S563
新クライアント用ルート鍵証明書＋更新要求
S564
S565
配布用ルート鍵証明書を用いて新クライアント用ルート鍵証明書の正当性を確認
S566
新クライアント用ルート鍵証明書を記憶し、配布用ルート鍵証明書、従前のクライアントルート鍵証明書を廃棄
結果通知
S567
結果通知
S568

【図４０】

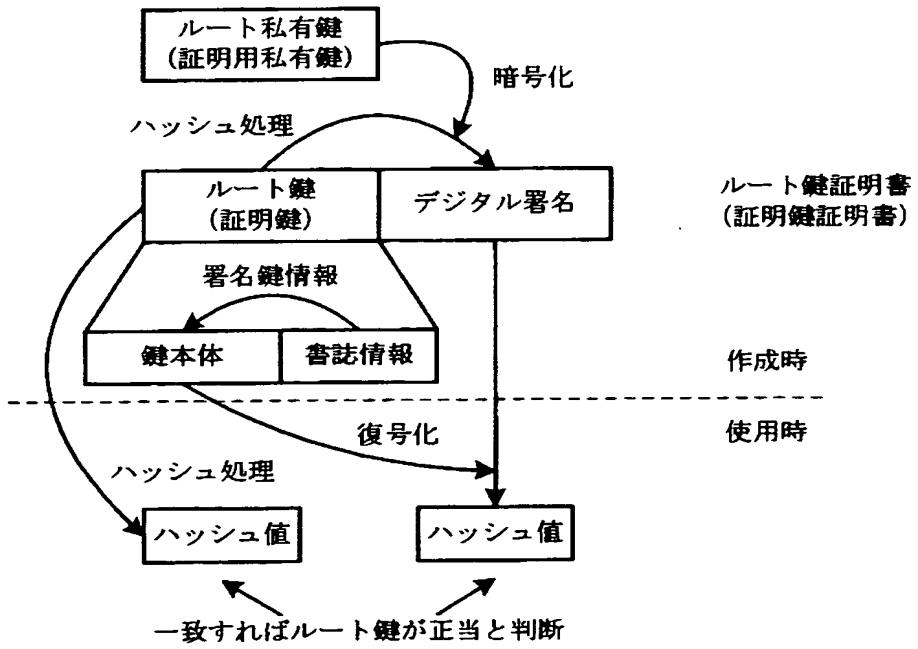

START
ルート鍵証明書
作成処理
（処理U）
クライアント装置の
ルート鍵証明書記憶処理
（処理３２）
サーバ装置の
公開鍵証明書記憶処理
（処理３４）
クライアント装置のルート鍵
証明書書き換え処理
（処理３６）
END

【図４１】

（ａ）


ルート私有鍵
(証明用私有鍵)
暗号化
ハッシュ処理
サーバ公開鍵
デジタル署名
サーバ公開鍵証明書
(サーバ証明書)
鍵本体
書誌情報
署名鍵情報
作成時
使用時
ハッシュ処理
復号化
ハッシュ値
ハッシュ値
ルート鍵本体
一致すればサーバ公開鍵が正当と判断

（ｂ）


ルート私有鍵
(証明用私有鍵)
暗号化
ハッシュ処理
ルート鍵
(証明鍵)
デジタル署名
ルート鍵証明書
(証明鍵証明書)
署名鍵情報
鍵本体
書誌情報
作成時
使用時
復号化
ハッシュ処理
ハッシュ値
ハッシュ値
一致すればルート鍵が正当と判断

【書類名】要約書
【要約】
【課題】　クライアント・サーバシステムにおける認証処理でデジタル証明書の正当性確認に用いるルート鍵を自動的に更新できるようにする。
【解決手段】　クライアント装置とサーバ装置との間で通信を確立する際に公開鍵暗号を利用したデジタル証明書を用いるＳＳＬ等の方式による認証を行い、その認証に伴って確立した通信経路で通信を行うようにしたクライアント・サーバシステムに、デジタル証明書管理装置を接続し、サーバ装置とクライアント装置のルート鍵を自動的に更新するデジタル証明書管理システムを構成する。そして、この更新処理において、サーバ装置に公開鍵証明書を送信する処理（処理４）を、クライアント装置に新ルート鍵を送信する処理（処理２）の後で行うようにする。
【選択図】　　図１３

特願２００４－０５６７６４

# 出願人履歴情報

識別番号　［０００００６７４７］

１．変更年月日　２００２年　５月１７日
［変更理由］　住所変更
住　所　東京都大田区中馬込１丁目３番６号
氏　名　株式会社リコー